AGENDA

REMOTE MEETING NOTICE

This meeting will be accessible by remote video conferencing. Please be advised that while the District will endeavor to ensure these remote participation methods are available, the District does not guarantee that they will be technically feasible or work all the time. Further, the District reserves the right to terminate these remote participation methods (Subject to Brown Act Restrictions) at any time and for whatever reason. The public may observe and participate in this meeting remotely via Zoom as set forth below.

INSTRUCTIONS FOR USING ZOOM

- Join the meeting using the link below.
- You must have audio and microphone capabilities on the device you are using to join the meeting.
- When you join the meeting make sure that you join the meeting with audio and follow the prompts to test your speaker & microphone prior to joining the meeting.

TO SPEAK DURING PUBLIC COMMENT USING ZOOM

- The Board President will announce when it is time for Public Comment.
- Click on the Raise Hand icon if you would like to speak during Public Comment.
- Your name will be called on when it's your turn to speak.
- When your name is called, you will be prompted to unmute yourself.
- You will have three (3) minutes to speak. When your time is up, you will be muted.

TO SPEAK ON AN ITEM USING ZOOM

- The Board President will call the item and staff will begin the staff report.
- Click on the Raise Hand icon if you would like to speak on the item.
- Your name will be called on when it's your turn to speak.
- When your name is called, you will be prompted to unmute yourself.
- You will have three (3) minutes to speak. When your time is up, you will be muted.
- You will repeat this process for each item you want to speak on.

FOR OPEN SESSION PARTICIPATION
Join Meeting Electronically at:

Join Zoom Meeting

https://us02web.zoom.us/j/87609460312?pwd=gRs7iIErhIKZ45C6YQB9a9Eo48yovt.1

Meeting ID: 876 0946 0312

Passcode: 197215

Please attend in person or by submitting your comment via email to:
RMangus@GoletaSanitary.Org

A G E N D A
REGULAR MEETING OF THE GOVERNING BOARD
OF THE GOLETA SANITARY DISTRICT
A PUBLIC AGENCY

One William Moffett Place
Goleta, California 93117

September 9, 2026

CALL TO ORDER: 3:00 p.m.

ROLL CALL OF MEMBERS

BOARD MEMBERS: Steven T. Majoewsky
Dean Nevins
Jonathan Frye
Edward Fuller
Joseph Glancy

CONSIDERATION OF THE MINUTES OF THE BOARD MEETING

The Board will consider approval of the Minutes of the Regular Meeting of August 17, 2026.

PUBLIC COMMENTS - Members of the public may address the Board on items within the jurisdiction of the Board. Under provisions of the Brown Act, the Board is prohibited from taking action on items not listed on the agenda. Please limit your remarks to three (3) minutes and if you wish, state your name and address for the record.

POSTING OF AGENDA – The agenda notice for this meeting was posted at the main gate of the Goleta Sanitary District and on the District's web site 72 hours in advance of the meeting.

BUSINESS:

1. CONSIDERATION OF POTENTIAL CAPITAL PROJECT FUNDING IMPACTS ASSOCIATED WITH GOLETA WEST SANITARY DISTRICT'S FISCAL YEAR 2026-27 BUDGET
(Board may take action on this item)

2. LINCOLN MULTI-FUND 457 PLAN TRANSFER TO LINCOLN ALLIANCE PROGRAM 457 PLAN

3. UPDATE ON THE DISTRICT'S CYBER SECURITY CONTROL STANDARDS

4. CONSIDERATION OF TRANSFERRING ADDITIONAL FUNDS FROM COMMUNITY WEST BANK ICS MONEY MARKET FUND TO CALIFORNIA

COOPERATIVE LIQUID ASSET SECURITIES SYSTEM (“CA-CLASS”) TERM SERIES II PORTFOLIOS
(Board may take action on this item)

5. GENERAL MANAGER’S REPORT

6. LEGAL COUNSEL'S REPORT

7. COMMITTEE/DIRECTOR'S REPORTS AND APPROVAL/RATIFICATION OF DIRECTOR’S ACTIVITIES

8. PRESIDENT'S REPORT

9. ITEMS FOR FUTURE MEETINGS

10. CORRESPONDENCE
(The Board will consider correspondence received by and sent by the District since the last Board Meeting.)

11. APPROVAL OF BOARD COMPENSATION AND EXPENSES AND RATIFICATION OF CLAIMS PAID BY THE DISTRICT
(The Board will be asked to ratify claims.)

12. CLOSED SESSION

(i) PUBLIC COMMENTS ON CLOSED SESSION ITEMS

(ii) PUBLIC EMPLOYMENT
Government Code Section 54957
Title: General Manager

(iii) CONFERENCE WITH LABOR NEGOTIATORS
Government Code 54957.6
Agency designated representatives: Personnel Committee Members
President Steve Majoewsky and Board member Jon Frye
Unrepresented employee: General Manager

ADJOURNMENT

Persons with a disability who require any disability-related modification or accommodation, including auxiliary aids or services, in order to participate in the meeting are asked to contact the District’s Finance Director at least 3 hours prior to the meeting by telephone at (805) 967-4519 or by email at info@goletasanitary.org.

Any public records which are distributed less than 72 hours prior to this meeting to all, or a majority of all, of the District’s Board members in connection with any agenda item (other than closed sessions) will be available for public inspection at the time of such distribution at the District’s office located at One William Moffett Place, Goleta, California 93117.

MINUTES

MINUTES
REGULAR MEETING OF THE GOVERNING BOARD
GOLETA SANITARY DISTRICT
A PUBLIC AGENCY
DISTRICT OFFICE CONFERENCE ROOM
ONE WILLIAM MOFFETT PLACE
GOLETA, CALIFORNIA 93117

August 17, 2026

CALL TO ORDER:	President Majoewsky called the meeting to order at 6:30 p.m.
BOARD MEMBERS PRESENT:	Steven T. Majoewsky, Dean Nevins, Jonathan Frye, Edward Fuller, Joseph Glancy
BOARD MEMBERS ABSENT:	None
STAFF MEMBERS PRESENT:	Steve Wagner, General Manager/District Engineer, Vyto Adomaitis, Assistant General Manager, Rob Mangus, Finance Director/Board Secretary, Reese Wilson, Engineering Manager, Laura Romano, Communications and Human Resources Manager and Jeff Ferre, General Counsel (via Zoom)
OTHERS PRESENT:	David Linville, Director, Goleta Water District (via Zoom) Tom Evans, Director, Goleta Water District (via Zoom) Craig Geyer, Director, Goleta West Sanitary District (via Zoom)
APPROVAL OF MINUTES:	Director Frye made a motion, seconded by Director Fuller, to approve the minutes, as corrected, of the Regular Board meeting of 08/03/2026. The motion carried by the following vote:

(26/08/2147)

AYES:	4	Majoewsky, Frye, Fuller, Glancy
NOES:		None
ABSENT:		None
ABSTAIN:	1	Nevins

POSTING OF AGENDA:	The agenda notice for this meeting was posted at the main gate of the Goleta Sanitary District and on the District's website 72 hours in advance of the meeting.
PUBLIC COMMENTS:	None

BUSINESS:

1. CONSIDERATION AND APPROVAL OF RESOLUTION NO. 26-741 ADOPTING FINDINGS, APPROVING THE CERTIFICATE OF DETERMINATION AND AUTHORIZING PREPARATION AND FILING OF NOTICE OF EXEMPTION UNDER CEQA FOR THE CHANNEL A SLUICE GATE REPLACEMENT PROJECT
   Mr. Adomaitis gave the staff report.

   Director Fuller made a motion, seconded by Director Nevins, to approve and adopt Resolution No. 26-741 Adopting findings, approving the certificate of Determination and authorizing preparation and filing of the Notice of Exemption under CEQA for the Channel A Sluice Gate Replacement Project.

   (26/08/2148)

AYES:	5	Majoewsky, Nevins, Frye, Fuller, Glancy
NOES:		None
ABSENT:		None
ABSTAIN:		None

2. CONSIDERATION OF PROPOSAL FOR THE CHANNEL A SLUICE GATE REPLACEMENT PROJECT
   Mr. Adomaitis and Mr. Wilson gave the staff report.

   Director Nevins made a motion, seconded by Director Frye, to approve the General Manager to enter into a construction contract with Cushman Contracting Corporation, in the amount of $75,000, for the Channel A Sluice Gate Replacement Project.

   (26/08/2149)

AYES:	5	Majoewsky, Nevins, Frye, Fuller, Glancy
NOES:		None
ABSENT:		None
ABSTAIN:		None

3. CONSIDERATION AND ADOPTION OF RESOLUTION NO. 26-742 AMENDING AND ADOPTING RECOMMENDED REVISIONS TO THE HUMAN RESOURCES PROCEDURE AND POLICY MANUAL
   Mr. Adomaitis and Ms. Romano gave the staff report.

   Director Nevins made a motion, seconded by Director Glancy, to approve and adopt Resolution No. 26-742 Amending and Adopting recommended revisions to the Human Resources Procedure and Policy Manual, with the changes noted during the meeting.

(26/08/2150)

AYES:	5	Majoewsky, Nevins, Frye, Fuller, Glancy
NOES:		None
ABSENT:		None
ABSTAIN:		None

4. CONSIDERATION OF BOARDROOM AUDIO VISUAL UPGRADES
Mr. Adomaitis and Mr. Wagner gave the staff report on this discussion item. The Board gave direction to staff to return with options for consideration.

5. GENERAL MANAGER'S REPORT
Mr. Adomaitis gave the report.

6. LEGAL COUNSEL'S REPORT
Mr. Ferre – No report.

7. COMMITTEE/DIRECTORS' REPORTS AND APPROVAL/RATIFICATION OF DIRECTORS' ACTIVITIES
Director Nevins – No report.

Director Frye – Reported on his attendance at the CASA Conference.

Director Fuller – Reported on his attendance at the CASA Conference.

Director Glancy – No report.

8. PRESIDENT'S REPORT
President Majoewsky – Submitted his report on the Goleta Water District meeting he attended.

9. ITEMS FOR FUTURE MEETINGS
There was Board consensus to arrange a tour for the Board of the Lystek project operation.

10. CORRESPONDENCE
The Board reviewed and discussed the list of correspondence to and from the District in the agenda.

11. APPROVAL OF BOARD COMPENSATION AND EXPENSES AND RATIFICATION OF CLAIMS PAID BY THE DISTRICT

Director Nevins made a motion, seconded by Director Fuller, to ratify and approve the claims, for the period 08/03/2026 to 08/17/2026 as follows:

Running Expense Fund #4640	$	588,403.29
Capital Reserve Fund #4650	$	11,719.55
Depreciation Replacement Reserve Fund #4655	$	28,705.96

The motion carried by the following vote:

(26/08/2151)

AYES:	5	Majoewsky, Nevins, Frye, Fuller, Glancy
NOES:		None
ABSENT:		None
ABSTAIN:		None

12. CLOSED SESSION

(i) PUBLIC COMMENTS ON CLOSED SESSION ITEM
No comment

(ii) DESIGNATION OF STEVE WAGNER, GENERAL MANAGER, AS DISTRICT REPRESENTATIVE FOR LABOR NEGOTIATIONS

(iii) CLOSED SESSION PURSUANT TO GOVERNMENT CODE SECTION 54957.6 - CONFERENCE WITH LABOR NEGOTIATOR REGARDING AGENCY DESIGNATED REPRESENTATIVE GENERAL MANAGER STEVE WAGNER UNREPRESENTED EMPLOYEES: ALL DISTRICT EMPLOYEES
(Board may take action on this item.)

Board entered closed session at 7:32 p.m.
Board returned to open session at 7:48 p.m.

There was no reportable action in Closed Session

ADJOURNMENT
There being no further business, the meeting was adjourned at 7:49 p.m.

ATTEST

Steven T. Majoewsky	Robert O. Mangus, Jr.
Governing Board President	Governing Board Secretary

AGENDA ITEM #1

AGENDA ITEM: 1

MEETING DATE: September 9, 2026

I. NATURE OF ITEM

Consideration of Potential Capital Project Funding Impacts Associated with Goleta West Sanitary District's Fiscal Year 2026-27 Budget

II. BACKGROUND INFORMATION

On August 21, 2026, staff was informed that the Goleta West Sanitary District (GWSD) Board approved their Fiscal Year 2026-27 (FY27) budget with a condition that they will not fund any non-mandated capital projects for FY27 to allow time to complete a financial analysis of their Force Main Replacement project.

While the replacement of the force mains is not required as part of GWSD's settlement agreement with the Central Coast Regional Water Quality Control Board for the sewer spill event that occurred in February of 2024, the project is needed to reduce the risk of future sewer system overflows into the Goleta Slough. As such, GWSD has made the timely completion of this project their top priority.

The total cost of GWSD's Force Main Replacement project is unknown at this time but could be $20M or more depending on the final scope of the project and pipeline alignment. It is staff's understanding that the cost of this project is the primary reason why GWSD included the restriction on capital project funding in the approval of their FY27 budget.

While GWSD's FY27 capital funding restriction is general, staff believes that the intent was to apply the restriction only to the District's Solids Handling Improvement Project (SHIP) and Energy Storage Project (ESP). There are several smaller capital projects that are included in the District's FY27 Budget which were presented to GWSD in May 2026. As such, staff has asked GWSD for further clarification on the funding restriction and duration.

As with any large-scale project, the effort and costs associated with getting the SHIP and ESP projects ready for construction have been considerable. The costs associated with delaying these projects could be significant based on the duration of the delay.

Staff is preparing two financial analyses: an analysis of the potential costs associated with delaying these projects and a financial analysis of moving forward with the projects without GWSD's near term financial participation. Staff will be working with Raftelis, as they developed our recent rate study which includes a capital funding model which can be adapted for this analysis.

The results of these analyses will be brought to the Board for consideration at a subsequent meeting and will be shared with GWSD.

III. COMMENTS AND RECOMMENDATIONS

A table showing the current construction schedule and estimated annual project costs associated with the SHIP and ESP is shown below. The table includes the estimated annual cost allocations for GWSD and GSD for these projects (excluding any grant funding).

	Estimated Project Costs				
Project Name	**FY27**	**FY28**	**FY29**	**FY30**	**4-Year Total**
Solids Handling Improvement Project	$1,750,000	$10,000,000	$9,500,000	$7,650,000	$28,900,000
Energy Storage Project	$3,520,000	$1,670,000			$5,190,000
Total	**$5,270,000**	**$11,670,000**	**$9,500,000**	**$7,650,000**	**$34,090,000**
GWSD CIP Cost Allocation (40.78%)	$2,149,106	$4,759,026	$3,874,100	$3,119,670	$13,901,902
GSD CIP Cost Allocation (47.87%)	$2,522,749	$5,586,429	$4,547,650	$3,662,055	$16,318,883
Total:	**$4,671,855**	**$10,345,455**	**$8,421,750**	**$6,781,725**	**$30,220,785**

GWSD has scheduled a Finance Committee meeting to discuss this issue on September 8, 2026. Staff will attend this meeting and provide a verbal report to the Board at a future meeting.

Staff will continue to work closely with GWSD to clarify the intent and duration of the capital funding restriction and identify ways to reduce the potential costs associated with delaying these projects.

IV. REFERENCE MATERIAL

None

AGENDA ITEM #2

AGENDA ITEM: 2

MEETING DATE: September 9, 2026

I. NATURE OF ITEM

Lincoln Multi-Fund 457 Plan Transfer to Lincoln Alliance Program 457 Plan

II. BACKGROUND INFORMATION

On August 16, 1982, the Board resolved to establish a deferred compensation plan under the Internal Revenue Code (IRC) Section 457 for its employees and authorized the execution of relevant agreements with Lincoln National Life Insurance Co. In subsequent years, the plan has been amended to add features, for example a Roth provision, or to comply with changes in IRC Section 457. The Lincoln Multi-Fund Variable Annuity Investment 457 Plan was very old, and the customer service for the plan was not satisfactory for both the administration of the plan, or for its participants.

III. COMMENTS AND RECOMMENDATIONS

Staff asked our Lincoln representative about these service issues, and the representative came back with a proposal to update the plan to Lincoln's Alliance Program which offers better interface platforms for both administration and participants. The switch was just completed, and we have a presentation scheduled for staff on September 10, 2026, at 2:00 p.m.

IV. REFERENCE MATERIAL

Lincoln Alliance 457 Plan Proposal

Lincoln Financial

RETIREMENT PLAN SERVICES

February 3, 2026

Why Lincoln retirement plans

Proposal prepared by Lincoln for:

Goleta Sanitary Water District

Dave Fernando Almeida

Osaic Wealth Inc.

2775 N Ventura Road, Suite 101

Oxnard, CA 93036

805-973-5917

LCN-7815977-040325

Lincoln invests in your success

Going above and beyond in service to you is our way of life.

We bring a personalized approach to retirement plan servicing through our unwavering dedication and breadth of experience:

Retirement and wellness

solutions holistically designed to enable more people to confidently succeed their way.

Service

that takes a consultative and deeply personal approach to supporting your plan and your people.

Technology

that drives measurable results through actionable information and customized experiences in line with your goals.

Benefits and services that deliver value

Pricing advantage for innovative solutions

These investment strategies and services can provide discounts if chosen for your plan. Your pricing summary displays the details about your specific proposed options.

Fiduciary services

Lincoln recognizes the dedication and sense of responsibility you feel for your organization and your employees. As a plan sponsor, you may already realize that your responsibilities extend to the legal realm, where laws governing retirement plans have specific provisions focused on plan fiduciary duties.

That's why we offer you access to services and support for navigating and managing your fiduciary role, helping you act in employees' best interest while easing the risk that comes with creating an investment strategy or selecting an investment lineup.

Mapping strategy and pricing

This summary is valid for 90 days from the proposal issue date.

Your plan details

Total plan assets	$2,940,047
Participants with a balance	17
Annual contributions	$78,855

[1]Pricing quote is based on plan valuation data provided. If actual plan characteristics vary from the assumptions at the time of plan establishment, the pricing will be adjusted accordingly. An additional $15 per participant charge may apply for plans with less than a $10,000 average account balance.

*Fees for 3(21) fiduciary lineup services are included in the pricing illustration under recordkeeping and servicing. See advisory services agreement for details.

§Pricing quote is based on fund mapping strategy. Initial Lincoln Stable Value allocation: 6%

|| Full-service plans: For loan administration, if applicable, there is a $100 loan initiation fee, $40 annual loan maintenance fee, $50 distribution processing fee, $40 in-service withdrawal fee, and a $750 QDRO processing fee.

Your plan pricing[1]

	Fund to fund*§||
Asset-based fees:	
Recordkeeping and servicing	0.36%
Compensation paid to your financial professional	0.40%
Total asset charge to participants	**0.76%**
Average fund expense	0.21%

Proposal for: Goleta Sanitary Water District
Date issued: 02/03/2026

Flexibility, choice, guidance, protection

Providing value for money spent

Here's what you need to know about the proposed options noted in your pricing summary.

A 3(21) investment fiduciary is a co-fiduciary on your plan, collaborating with you on your investment strategy and providing guidance on the plan's investment menu.

The investment lineup chosen for your plan delivers ERISA 3(21) fiduciary support from Morningstar Investment Management LLC. Along with offering your participants a diversified fund lineup, Morningstar provides a customized Investment Policy Statement, ongoing investment monitoring and reporting through quarterly watch lists, and a rigorous investment selection process with documents describing methodology for your reference and fiduciary files.

In a fund-to-fund strategy, participants' investments are mapped from the lineup you offer in your current plan to comparable funds — like for like — in your Lincoln lineup.

LCN-7815977-040325

A dedicated support system

Helping make your job easier

Lincoln Financial

The right team for all your needs

- Account and relationship management
- Implementation services
- Retirement consultant services (RC)

Handling the many tasks associated with running your plan

- Administration, recordkeeping, oversight
- Compliance and plan design services
- Continuous link between payroll and other plan data — integration with premier partners

Proactive plan design from day 1

Experienced and dedicated team

97% → Overall satisfaction with account and relationship management[1]

Overall satisfaction among plan sponsors[1] → 92%

91% → Overall satisfaction with the implementation partners[2]

Personalized service each time you call — and as the plan grows or goals change, your support evolves, too.

[1]Lincoln Financial, "Plan Sponsor Survey Results," 1Q 2025.
[2]Lincoln Financial, "RPS Post-implementation Survey," Fiscal year 2024.

Hands-on expertise and oversight

Achieving retirement plan success together

The people dedicated to your plan take the time to understand your goals, work through your challenges and find solutions that encourage the best possible outcomes for your company and your employees.

Your dedicated account manager	Your account manager serves as your single point of contact for administrative services requests and day-to-day plan operation. Lincoln's experienced team of account managers work in close partnership with your financial professional to deliver an outstanding customer service experience.
Plan administration and compliance services from seasoned professionals	Lincoln's experienced team of retirement plan specialists provide a broad variety of plan services, including comprehensive plan design consulting, document maintenance, plan reporting, and recordkeeping and transaction processing.

Knowledge, awareness and assistance

Inspiring smart saving behavior

Support when and how participants need it

Retirement consultants (RCs) provide in-person or virtual hands-on educational support in group and one-on-one meetings to help participants:

- Enroll in the plan
- Review an account or asset allocations
- Discuss contribution strategy and questions
- Answer account questions

Customized education program

A blend of communications and resources deliver the essential information employees need to make informed decisions and quickly take action on their terms — from enrollment through retirement.

- Mobile apps
- Print and email communication campaigns
- Comprehensive online tools

Participant communication recognition

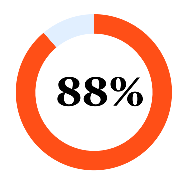
13 years running

Pensions & Investments (P&I) Eddy Award for Excellence in Employee Communications[1]

9 years of recognition

over the past decade, Plan Sponsor Council of America (PSCA) Signature Award for Excellence[2]

Participants contribute **77% more** when they **meet with an RC**[3]



of participants **meet or exceed the company match** when they **meet with an RC**[3]

[1]https://www.pionline.com/topic/eddy-awards
[2]https://www.psca.org/industry-intel/signature-awards
[3]Lincoln Financial Plan Data, 4Q 2024.

Intuitive, customized tools

Delivering measurable data and results

Winner of the **2024 DALBAR Web Communications Seal**[1]

Employer website

Helps you measure plan health, track employee progress and improve results.

- Key performance indicators (KPIs)
- Real-time plan analytics
- Benchmarking

53% higher deferral rates for web-engaged participants than non-web users.[2]

Employee website

Helps motivate them to take action to be retirement ready.

- Simplified voluntary and automatic enrollment and escalation experience
- Real income numbers
- Quick contribution increases
- Comprehensive account details

80% increase in deferral rates for Lincoln *WellnessPATH*® users[3]

Holistic financial wellness tool

Provides resources and insight into short- and long-term financial goals for a complete financial health picture.

- Actionable content, like gamified tools and checklists
- 1:1 support
- Personalized, interactive tools, like budgeting and account aggregation

[1] https://dalbar.com/Awards/AwardHistory.
[2] Lincoln Financial Plan Data, 1Q 2025.
[3] Participants registered for Lincoln *WellnessPATH*® April 1, 2024, through March 31, 2025, who increased their deferral rates within three months of signing up for *WellnessPATH*.

A partner you can feel good about

Lincoln Financial

Inspiring confidence in the choices you make for your retirement plan and your employees

We lead with strength, experience and purpose

100%
U.S.-based company,
in business since **1905**

We've been in the retirement industry for **more than** 60 years.

$109B+ in retirement plan assets[1]

We serve 1.7M+ participants across 22,000+ plans.[1]

We have 10 years of consecutive positive net flows.[2]

We hold ourselves to the **highest ethical and regulatory standards** and are **100% transparent** about our financial performance and leadership.

The Lincoln National Life Insurance Company (Fort Wayne, IN) and Lincoln Life & Annuity Company of New York (Syracuse, NY) ratings [3]

A.M. Best: **A (3rd highest of 16)**	Moody's: **A2 (6th highest of 21)**
Fitch: **A+ (5th highest of 19)**	S&P: **A+ (5th highest of 21)**

We make a meaningful impact

Member of Dow Jones Sustainability Indices In Collaboration with RobecoSAM

Ethisphere World's Most Ethical Companies 2022 - 2025

America's Most Responsible Companies 2024 Newsweek statista

Eagles Autism Challenge presented by Lincoln Financial

World's Most Trustworthy Companies 2023 Newsweek statista

[1]Lincoln Financial Book of Business, 1Q 2025.

[2]Lincoln Financial, as of 4Q 2024, https://www.lincolnfinancial.com/pbl-static/pdf/IR---Earnings-4Q2024-Conference---statistical-supplement---PDF.pdf

[3]These ratings apply only to the claims-paying ability of the issuing insurance company as of May 7, 2025. They do not apply to the safety or investment performance of any variable products or funds. The ratings do not imply approval of the variable products or their performance. All ratings are subject to revision or withdrawal at any time by the rating agencies. The ratings are not recommendations to buy, sell or hold our securities. While ratings can be objective indicators of an insurance company's financial strength and can provide a relative measure to help select among insurance companies, they are not guarantees of the future financial strength and/or claims paying ability of a company. For more information on ratings, including rating agency outlooks, see www.lincolnfinancial.com/public/aboutus/investorrelations/financialinformation/ratings.

An inclusive approach

Delivering more choice for you and results for your employees

Lincoln Financial

AB
Allspring
American Century Investments
BAIRD
BARON CAPITAL
BlackRock
CAPITAL GROUP | AMERICAN FUNDS
COLUMBIA THREADNEEDLE INVESTMENTS
Dimensional
EatonVance Investment Managers
Federated Hermes
Fidelity Investments
FRANKLIN TEMPLETON INVESTMENTS
Goldman Sachs | Asset Management
GREAT GRAY TRUST COMPANY
HARTFORDFUNDS
Invesco
Janus Henderson INVESTORS
John Hancock
J.P.Morgan Asset Management
LORD ABBETT
MACQUARIE
MFS
NATIXIS INVESTMENT MANAGERS
NEUBERGER | BERMAN
nuveen A TIAA Company
PIMCO
Principal
Prudential Investments
Putnam INVESTMENTS
stadion start smart. finish strong.
STATE STREET GLOBAL ADVISORS
T.RowePrice INVEST WITH CONFIDENCE
Vanguard
VictoryFunds
VIRTUS INVESTMENT PARTNERS

More than a retirement plan

Making a proven impact

[We invest in your success]

[We are in service of your success]

[We help you prioritize employees' financial wellness]

This is why people like working with us.

We hope you'll be one of them.

Disclosures

Mutual funds in the *Lincoln Alliance*® program are sold by prospectus. An investor should consider carefully the investment objectives, risks, and charges and expenses of the investment company before investing. The prospectus and, if available, the summary prospectus contain this and other important information and should be read carefully before investing or sending money. Investment values will fluctuate with changes in market conditions so that, upon withdrawal, your investment may be worth more or less than the amount originally invested. Prospectuses for any of the mutual funds in the *Lincoln Alliance*® program are available at 800-234-3500.

The *Lincoln Alliance*® program includes certain services provided by Lincoln Financial Advisors Corp. (LFA), a broker-dealer (member FINRA, SIPC) and retail and financial planning affiliate of Lincoln Financial Group, 1301 S. Harrison St., Fort Wayne, IN 46802. Unaffiliated broker-dealers also may provide services to customers. Account values are subject to fluctuation, including loss of principal.

Lincoln Financial Group® affiliates, their distributors, and their respective employees, representatives, and/or insurance agents do not provide tax, accounting, or legal advice. Please consult an independent professional as to any tax, accounting, or legal statements made herein.

There is no additional tax-deferral benefit for an annuity contract purchased in an IRA or other tax-qualified plan.

Choosing and periodically reviewing a plan's investment lineup is a fiduciary act. Lincoln is not proposing any particular lineup and is not acting as a fiduciary.

The Lincoln Stable Value Account is a fixed annuity contract issued by The Lincoln National Life Insurance Company, Fort Wayne, IN 46802 on Form 28866-SV 01/01, 28866-SV20 05/04, 28866-SV90 05/04, AN 700 01/12, or AR 700 10/09. **Guarantees for the Lincoln Stable Value Account are subject to the claims-paying ability of the issuer.**

The Lincoln NY Stable Value Account is a group fixed annuity contract issued by Lincoln Life & Annuity Company of New York, Syracuse, NY 13202 on Form AN 700NY 01/14 or AR 700NY 10/09. **Guarantees for the Lincoln NY Stable Value Account are subject to the claims-paying ability of the issuer.**

This material is provided by The Lincoln National Life Insurance Company, Fort Wayne, IN, and, in New York, Lincoln Life & Annuity Company of New York, Syracuse, NY, and their applicable affiliates (collectively referred to as "Lincoln"). This material is intended for general use with the public. Lincoln does not provide investment advice, and this material is not intended to provide investment advice. Lincoln has financial interests that are served by the sale of Lincoln programs, products, and services.

Morningstar Investment Management LLC is a registered investment adviser and subsidiary of Morningstar, Inc. Neither Morningstar Investment Management nor Morningstar, Inc. is affiliated with the Lincoln Financial Group. The Morningstar name and logo are registered marks of Morningstar, Inc. Morningstar Investment Management LLC, 22 W. Washington Street, Chicago, IL 60602.

Morningstar Investment Management LLC's investment lineups are subject to change. The investment options within a lineup do involve risk and will not always be profitable. Morningstar Investment Management does not guarantee that negative returns can or will be avoided in the lineups. An investment made in an investment option may differ substantially from its historical performance and, as a result, your plan participant may incur a loss. Past performance is no guarantee of future results.

The Morningstar Insight Series is not an investment option. It is a series of fund lineups chosen by Morningstar Investment Management LLC from the universe of investment options available in the *Lincoln Alliance*® program. Morningstar Investment Management LLC is a registered investment adviser and subsidiary of Morningstar, Inc. Neither Morningstar Investment Management nor Morningstar, Inc. is affiliated with the Lincoln Financial Group. The Morningstar name and logo are registered marks of Morningstar, Inc. Morningstar Investment Management LLC, 22 W. Washington Street, Chicago, IL 60602.

Morningstar Investment Management LLC is a leading independent provider of asset allocation, manager selection, and portfolio construction services. Morningstar Investment Management LLC is a registered investment adviser and subsidiary of Morningstar, Inc. Morningstar Investment Management and its affiliates are not an affiliate of Lincoln Financial Group.

Selection of a third party fiduciary is subject to fiduciary requirements under Section 404(a) of the Employee Retirement Income Security Act of 1974, as amended (ERISA). This brochure is meant to provide a plan sponsor with information regarding fiduciary services offered by Morningstar Investment Management LLC, but it is not intended to be and should not be construed as a recommendation by Lincoln. Plan sponsors should carefully evaluate any third party fiduciary prior to hiring the fiduciary. If the plan sponsor determines to appoint Morningstar Investment Management LLC as a 3(21) or 3(38) fiduciary, the plan sponsor is required to monitor Morningstar Investment Management LLC to assure that it is handling the plan's investments prudently and in accordance with the appointment.

Not a deposit
Not FDIC-insured
May go down in value
Not insured by any federal government agency
Not guaranteed by any bank or savings association

Lincoln Financial is the marketing name for Lincoln National Corporation and its affiliates.

Affiliates are separately responsible for their own financial and contractual obligations.

LincolnFinancial.com

AGENDA ITEM #3

AGENDA ITEM: 3

MEETING DATE: September 9, 2026

I. NATURE OF ITEM

Update on the District's Cyber Security Control Standards

II. BACKGROUND INFORMATION

The District relies on a wide range of computer technologies and systems to provide wastewater collection, treatment, and disposal services to the Goleta Valley. As the prevalence of cyber-attacks continues to increase across all business sectors, the risk of cyber-related attacks on the District's computer systems also continues to increase. Cyber security and risk mitigation have been common topics at recent wastewater industry seminars and conferences.

The 2025 Annual Report, presented to the Board in April 2026, contained an update on IT and Cyber Security measures that have been completed or were in process at that time. An excerpt from the 2025 Annual Report outlining these efforts is attached.

The District previously adopted the Center for Internet Security's (CIS) control standards in 2019 to improve its cyber security. The CIS publishes the Critical Security Controls (CSC) to help organizations better defend against known attacks by distilling key security concepts into actionable controls to achieve greater overall cyber security defense. The California Sanitation Risk Management Authority has also recommended that agencies implement the CIS controls to reduce cyber security risk.

CSC prioritizes and focuses on a small number of actions with high pay-off results. CSCs are effective because they are derived from the most common attack patterns identified in the leading threat reports and vetted across a broad community of government and industry practitioners. The list of CSCs was created by a group of cyber security experts from the NSA, the US Department of Energy's nuclear energy labs, law enforcement organizations, and some of the nation's top forensics and incident response organizations. CSCs are updated on an ongoing basis, based on new attacks that are identified and analyzed.

The District recently upgraded from CSC version 7 to CSC version 8.1, which consists of 18 cyber security controls containing 153 safeguards. The current framework uses Implementation Groups (IG1, IG2, and IG3) to prioritize implementation based on organizational risk, complexity, resources, and security needs. The District's cyber security efforts are focused initially on Implementation Group 1 (IG1), which CIS defines as the essential cyber hygiene baseline that every organization should implement.

The District has made significant progress in establishing technical and administrative safeguards, including asset and software management, secure configuration, account and access management, vulnerability and patch management, malware protection, data recovery, network security, security awareness, and incident response. Beyond these actions, staff is working to upgrade the District’s network monitoring and protection systems to help keep computers and data safe. The new systems will simplify security management and improve threat detection and investigation. The upgrades include implementation of the following:

- Network monitoring system
- Cyber Security Awareness Program
- Upgraded computer systems protection
- Network security stress tests to expose potential vulnerabilities

An assessment was carried out to establish a baseline for identifying remaining gaps, prioritizing remediation activities, and measuring future improvements in the District's cyber security. Of the 56 IG1 safeguards identified in CIS Controls version 8.1 which are applicable to the District, 23 are fully implemented, 18 are partially implemented, and 15 are pending validation.

CIS Controls are not intended to be a one-time project. The District will continue to review, maintain, and improve its implementation of the safeguards as technology, cyber security threats, regulatory requirements, and the District's environment evolves.

III. COMMENTS

This report is for informational purposes only. As such, no Board action is required.

IV. REFERENCE MATERIALS

CIS Controls Version 8.1 Controls Guide
CIS Controls Implementation
CIS Controls Status Report
District Cyber Security Activities Excerpt from 2025 Annual Report

CIS Critical Security Controls®

Version 8.1

March 2025

Center for Internet Security®

CIS Controls™

Acknowledgments

CIS would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Creative Commons License

March 2024

Contents

Overview

CIS Critical Security Controls

Appendix

Overview

Introduction

The CIS Critical Security Controls® (CIS Controls®) started as a simple grassroots activity to identify the most common and important real-world cyber attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and then share that information with a wider audience. The original goals were modest—to help people and enterprises focus their attention and get started on the most important steps to defend themselves from the attacks that really mattered.

Led by the Center for Internet Security® (CIS®), the CIS Controls have matured into an international community of volunteer individuals and institutions that:

- Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action
- Create and share tools, working aids, and stories of adoption and problem-solving
- Map the CIS Controls to regulatory and compliance frameworks in order to ensure alignment and bring collective priority and focus to them
- Identify common problems and barriers (like initial assessment and implementation roadmaps), and solve them as a community

The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls.

Evolution of the CIS Controls

The CIS Controls started like many similar activities; we gathered experts together, and shared and argued until we reached an agreement. This can be very valuable, depending on the people at the table and their experience. Through documenting and sharing the output, all enterprises can benefit from the work of people they cannot hire or even meet. You can improve the outcome (and your confidence in it) through selecting experts that represent a wide range of knowledge, bringing consistency to the process, and ensuring use of the best-available information (especially about attacks). In the end, you are still depending on the good judgment of a relatively small group of people, captured in an informal and narrative way.

At CIS, we have been on a multi-year path to bring more data, rigor, and transparency to the process of best practice recommendations (the CIS Benchmarks® and the CIS Controls). All of these elements are essential to the maturation of a science to underlie cyber defense; and, all are necessary to allow the tailoring and "negotiation" of security actions applicable in specific cases, and as required through specific security frameworks, regulations, and similar oversight schemes.

In the earliest versions of the CIS Controls, we used a standard list of publicly known attacks as a simple and informal test of the usefulness of specific recommendations. Starting in 2013, we worked with the Verizon Data Breach Investigations Report (DBIR) team to map the results of their large-scale data analysis directly to the CIS Controls, as a way to match their summaries of attacks into a standard program for defensive improvement.

CIS has recently released the **Community Defense Model (CDM)**, which is our most data-driven approach so far. In its initial version, the CDM looks at the conclusions from the most recent Verizon DBIR, along with data from the **Multi-State Information Sharing and Analysis Center® (MS-ISAC®)**, to identify what we believe to be the five most important types of attacks. We describe those attacks using the **MITRE Adversarial Tactics, Techniques, and Common Knowledge® (MITRE ATT&CK®) Framework** in order to create attack patterns (or specific combinations of Tactics and Techniques used in those attacks). This allows us to analyze the value of individual defensive actions (i.e., Safeguards[1]) against those attacks. Specifically, it also provides a consistent and explainable way to look at the security value of a given set of defensive actions across the attacker's life cycle, and provide a basis for strategies like defense-in-depth. The details of this analysis are available on the CIS website. The bottom line is that we have taken a major step toward identifying the security value of the CIS Controls, or any subset of them. While these ideas are still evolving, at CIS we are committed to the idea of security recommendations based on data, presented transparently. For additional information, reference **https://www.cisecurity.org/controls/v8-1/**.

These activities ensure that the CIS Security Best Practices (which include the CIS Controls and CIS Benchmarks) are more than a checklist of "good things to do," or "things that *could* help"; instead, they are a prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements.

[1] "Safeguards" were known as "Sub-Controls" prior to Version 8 of the CIS Controls.

This Version of the CIS Controls

CIS Controls version 8.1 (v8.1) is an iterative update to version 8.0. As part of our process to evolve the CIS Controls, we establish "design principles" that guide us through any minor or major updates to the document. Our design principles for this revision are context, clarity, and consistency. Context enhances the scope and practical applicability of Safeguards by incorporating specific examples and additional explanations. Coexistence aligns with other major security frameworks to the extent practical, while preserving the unique features of the CIS Controls. Consistency maintains continuity for existing CIS Controls users, ensuring little to no change due to this update. Here are the broad changes we've made for each design principle:

- **Context**
  - We've updated the CIS Controls with new asset classes to better match the specific parts of an enterprise's infrastructure each Safeguard applies to. New classes require new definitions, so we've also enhanced the descriptions of several Safeguards for greater detail, practicality, and clarity.
- **Coexistence**
  - The CIS Controls has always maintained alignment with evolving industry standards and frameworks and will continue to do so. This assists all users of the Controls and is a core principle of how the Controls operate. The release of NIST's CSF 2.0 necessitated updated mappings and updated security functions.
- **Consistency**
  - Traditionally any iterative update to the CIS Controls should minimize disruption to Controls users. This means that no Implementation Groups were modified in this update, and the spirit of any given Safeguard remains the same. Additionally, the new asset classes and definitions needed to be consistently applied throughout the Controls, and in doing so some minor updates were added.

With these principles in mind, we've scoped the CIS Controls v8.1 to the following updates:

- Realigned NIST CSF security function mappings to match NIST CSF 2.0
- Included new and expanded glossary definitions for reserved words used throughout the Controls (e.g., plan, process, sensitive data)
- Revised asset classes, alongside new mappings to Safeguards
- Fixed minor typos in Safeguard descriptions
- Added clarification to a few anemic Safeguard descriptions

One key improvement to CIS Controls v8.1 mapping is the addition of the "Governance" security function. Effective governance provides the structure needed to steer a cybersecurity program toward achieving their enterprise goals. The Controls were designed to be comprehensive enough to protect and defend cybersecurity programs for any size enterprise, while being prescriptive enough to ease implementation. With the update to CIS Controls v8.1, governance topics are now specifically identified as recommendations that can be implemented to enhance the governance of a cybersecurity program. This will help our adopters better identify the governing pieces of the program as well as equip them with the evidence needed to demonstrate compliance.

The CIS Controls aim to streamline the process of designing, implementing, measuring, and managing enterprise security. This involves simplifying language to reduce duplication, focusing on measurable actions with defined metrics, and ensuring each Safeguard is clear and concise. CIS continues to balance the need to address current cybersecurity challenges with maintaining a stable, foundational cyber defense strategy, steering clear of overly complex or inaccessible technologies. Technology is constantly shifting, and the CIS Controls team is aware of the developments in artificial Intelligence, augmented reality, and ambient computing working to reshape our enterprise infrastructure in subtle and radical ways. We're keeping both eyes open and already working on ideas for version 9 of the CIS Controls.

The CIS Controls Ecosystem ("It's not about the list")

Whether you use the CIS Controls, and/or another way to guide your security improvement program, you should recognize that "it's not about the list." You can get a credible list of security recommendations from many sources—it is best to think of the list as a starting point. It is important to look for the ecosystem that grows up around the list. Where can I get training, complementary information, explanations; how have others implemented and used these recommendations; is there a marketplace of vendor tools and services to choose from; how will I measure progress or maturity; how does this align with the myriad regulatory and compliance frameworks that apply to me? The true power of the CIS Controls is not about creating the best list, it is about harnessing the experience of a community of individuals and enterprises to actually make security improvements through the sharing of ideas, tools, lessons, and collective action.

To support this, CIS acts as a catalyst and clearinghouse to help us all learn from each other. Since Version 6, there has been an explosion of complementary information, products, and services available from CIS, and from the industry-at-large. Please email **controlsinfo@cisecurity.org** for the following kinds of working aids and other support materials:

- Mappings from the CIS Controls to a very wide variety for formal Risk Management Frameworks (like NIST®, Federal Information Security Modernization Act (FISMA), International Organization for Standardization (ISO), etc.)
- Use cases of enterprise adoption

- A list of ongoing references to the CIS Controls in national and international standards, state and national legislation and regulation, trade and professional associations, etc.
- Information tailored for small and medium enterprises
- Measurement and metrics for the CIS Controls
- Pointers to vendor white papers and other materials that support the CIS Controls
- Documentation on alignment with the NIST® Cybersecurity Framework

How to Get Started

Historically, the CIS Controls were ordered in sequence to focus an enterprise's cybersecurity activities, with a subset of the first six CIS Controls referred to as "cyber hygiene." However, this proved to be too simplistic. Enterprises, especially small ones, could struggle with some of the early Safeguards and never get around to implementing later CIS Controls (for example, having a backup strategy to help recover from ransomware). As a result, starting with Version 7.1, we created CIS Controls **Implementation Groups (IGs)** as our recommended new guidance to prioritize implementation.

The CIS Controls IGs are self-assessed categories for enterprises. Each IG identifies a subset of the CIS Controls that the community has broadly assessed to be applicable for an enterprise with a similar risk profile and resources to strive to implement. These IGs represent a horizontal look across the CIS Controls tailored to different types of enterprises. Specifically, we have defined IG1 as "essential cyber hygiene," the foundational set of cyber defense Safeguards that every enterprise should apply to guard against the most common attacks (**https://www.cisecurity.org/controls/v8-1/**). Each IG then builds upon the previous one: IG2 includes IG1, and IG3 includes all CIS Safeguards in IG1 and IG2.

Using or Transitioning from Prior Versions of the CIS Controls

As the cyber threat landscape is continuously changing, we believe Version 8 and any updates are the best comprehensive controls we have ever produced. We also appreciate that enterprises who are actively using prior versions of the CIS Controls as a key part of their defensive strategy might be reluctant to move to Version 8. Our recommendation is that if you are using Version 7 or Version 7.1, you are following an effective and usable security plan, and over time you should consider moving to the latest iteration. If you are using Version 6 (or earlier), our recommendation is that you should start to plan a transition to Version 8 as soon as practicable.

For prior versions of the CIS Controls, we were able to provide only the simplest tools to aid in transition from prior versions, basically a spreadsheet-based change log. For Version 8, we have taken a much more holistic approach and worked with numerous partners to ensure that the CIS Controls ecosystem is ready to support your transition, https://www.cisecurity.org/controls/v8-1/.

Structure of the CIS Controls

The presentation of each Control in this document includes the following elements:

- **Overview.** A brief description of the intent of the Control and its utility as a defensive action
- **Why is this Control critical?** A description of the importance of this Control in blocking, mitigating, or identifying attacks, and an explanation of how attackers actively exploit the absence of this Control
- **Procedures and tools.** A more technical description of the processes and technologies that enable implementation and automation of this Control
- **Safeguard descriptions.** A table of the specific actions that enterprises should take to implement the Control

Implementation Groups

IG1

An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

IG2 (Includes IG1)

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

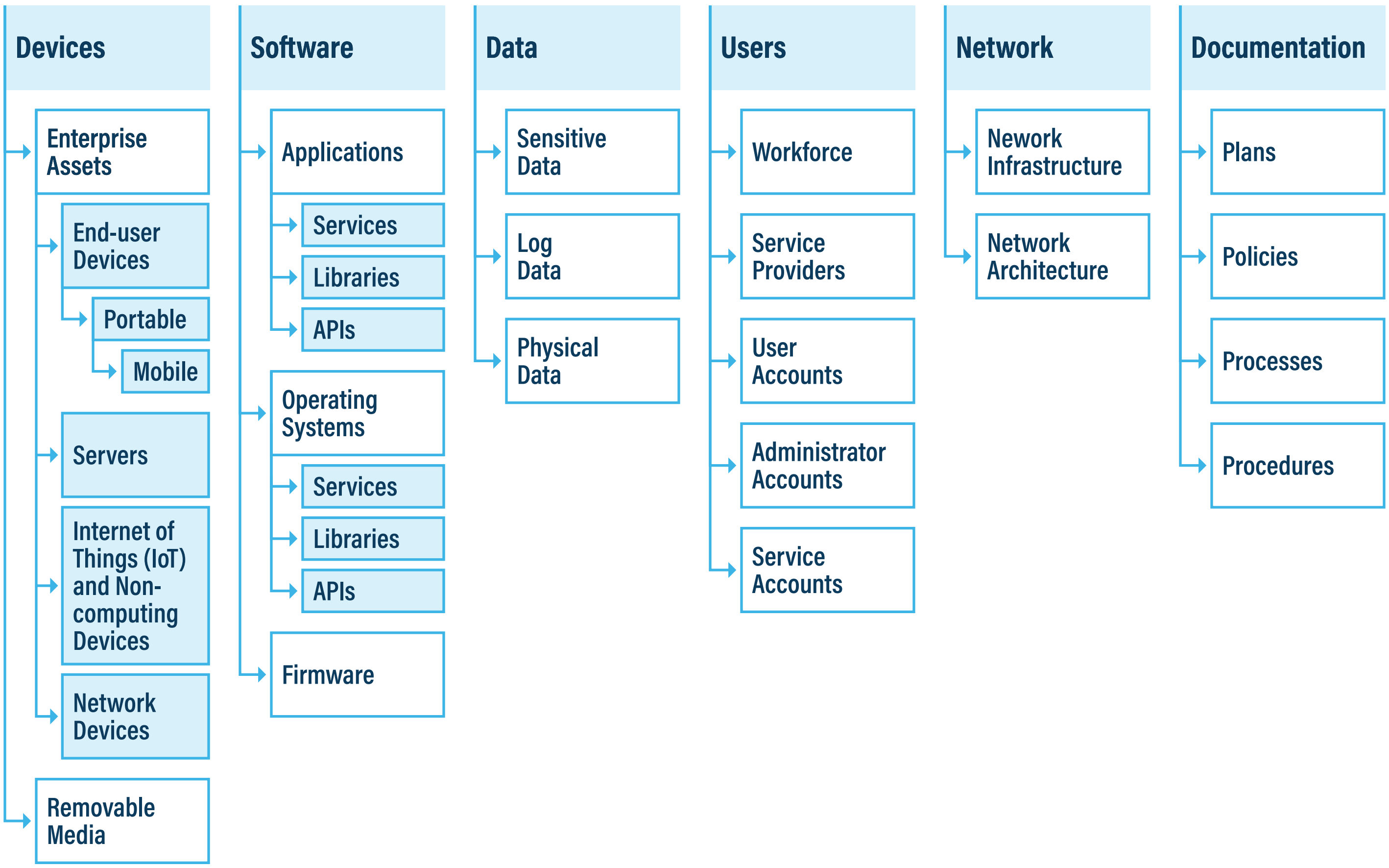
Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3 (Includes IG1 and IG2)

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

Asset Classes



Devices

Devices are enterprise assets (data processing and storage assets), end-user devices, portable devices, mobile devices, servers, Internet of Things and non-computing devices, network devices, and removable media. Devices may exist in physical spaces, virtual infrastructure, or cloud-based environments. Devices can remotely connect to these systems.

- **Enterprise Assets:** Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments.
  - **End-user Devices:** Information technology (IT) assets used among members of an enterprise during work or off-hours. End-user devices include desktops and workstations, as well as portable and mobile devices such as laptops, smartphones, and tablets. For the purpose of this document, end-user devices are a subset of enterprise assets.

- **Portable Devices:** Transportable, end-user devices that have the capability to wirelessly connect to a network. Portable devices can include laptops which may require external hardware for connectivity and mobile devices, such as smartphones and tablets. For the purpose of this document, portable devices are a subset of end-user devices.
  - **Mobile Devices:** Small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. For the purpose of this document, mobile devices are a subset of portable devices.
- **Servers:** A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Servers can exist in datacenters, public/private/hybrid cloud environments, including temporal containers or serverless workloads. Examples of servers include web servers, application servers, mail servers, and file servers. For the purpose of this document, servers are a subset of enterprise assets.
- **Internet of Things (IoT) and Non-computing Devices:** Devices embedded with sensors, software, and other technologies. These devices may connect, store, and exchange data with other devices and systems. The device's connection to the internet can be intermittent, non-existent, or persistent. Examples of these devices include smart watches and other wearables, printers, smart screens, smart home devices, speakers, industrial control systems, and physical security sensors. For the purpose of this document, IoT and non-computing devices are a subset of enterprise assets.
- **Network Devices:** Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware, as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets. Note that network devices are listed under Enterprise Assets because they are managed much like other devices, however, they also play a dual role in the Network Asset Class when related to the communication over a network.

- **Removable Media:** Any type of storage device that can be removed from a computer while the system is running and allows data to be moved from one system to another. Examples of removable media include CDs, DVDs, Blu-ray Discs, external hard drives, SD cards, tape backups, diskettes, and USB drives.

Software

Sets of data and instructions used to direct a computer to complete a specific task. Software assets include operating systems and applications. Both may contain services, libraries, or Application Programming Interfaces (APIs).

- **Applications:** A program, or a group of programs, running on top of an operating system hosted on an enterprise asset. Example application types include web, database, cloud-based, and mobile. Applications are considered a software asset in this document.
- **Operating Systems:** Software on enterprise assets that manages computer hardware and software resources and provides common services for programs. Example operating systems include Windows, Ubuntu, MacOS, Android, and z/OS. Operating systems are considered a software asset.
  - **Services:** Specialized programs that perform well-defined critical tasks for the operating system. Services often start with the operating system, run-in in the background, and can be stopped and started by users. Example services include managing network communications, users, file permissions, system security, and device interaction.
  - **Library:** A shareable pre-compiled codebase to include classes, procedures, scripts, configuration data, and more, used to develop software programs and applications. Libraries are designed to assist both the programmer and the programming language compiler in building and executing software more efficiently.
  - **Application Programming Interface (API):** A set of rules and interfaces for software components to interact with each other in a standardized way. APIs allow applications to access and communicate with both internal and external resources.
- **Firmware:** Software stored within a device's non-volatile memory, such as ROM or flash memory, used to allow different types of hardware to communicate with the operating system. Firmware is often updated outside of the enterprise's operating system and application software update process.

Data

A collection of facts that can be examined, considered, and used for decision-making. Although data may be physical, the CIS Controls primarily provide protection for digital data that may be stored, transferred, and processed by enterprise assets.

- **Sensitive Data:** Physical or digital data stored, processed, or managed by the enterprise that must be kept private, accurate, reliable, and available. If released or destroyed in an unauthorized manner, it would cause harm to the enterprise or its customers. These impacts may be due to a data breach or a violation of a policy, contract, or regulation.
- **Log Data:** A computer-generated data file that records the events occurring within the enterprise. Examples of logs include: operating system, anti-malware detection, database, application, network, firewall, web server, or access control logs (e.g., electronic locks, alarm system).
- **Physical Data:** Data that is stored in physical documents or stored on physical types of removable devices (e.g., USB drives, tape backups). Physical data may be sensitive or not.

Users

Employees, third-party vendors, contractors, service providers, consultants, or any other person who is authorized to access an enterprise asset. This also includes user, administrator, and service accounts.

- **Workforce:** All individuals who are employed or engaged by an organization and have access to its information systems, assets, or resources. It includes all employees both on-site and remote, excluding service providers and consultants.
- **Service Providers:** Entity that offers platforms, software, and services to other enterprises. Examples include IT consultants, managed service provider (MSPs), Software as a Service (SaaS) platforms, and cloud service providers. Third-party providers and vendors are also considered Service Providers. These services may be paid or free. Some relationships may or may not require a contract or SLA in place. Examples include data analysis, traffic blocking, and similar services.
- **User Accounts:** An identity comprised of a set of credentials (e.g., username, password) that defines a user on a computer or computing system. A user account keeps track of a user's information and settings, controls the files, folders, and resources a user is allowed to access, as well as the tasks a user is allowed to perform. For the purpose of this document, user accounts refer to "standard" user accounts with limited privileges and are used for general tasks.
- **Administrator Accounts:** Accounts for users requiring escalated privileges. The accounts are used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure. Each administrator account should be assigned to a single user. Common administrator account subtypes include root accounts, local administrator, domain administrator accounts, and network or security appliance administrator accounts.
- **Service Accounts:** A service account is created specifically to run applications, services, and automated tasks on an operating system. Service accounts may also be created just to own data and configuration files. Each service account should be used for a specific service or function, and it should have an assigned owner who is responsible for how the account is used. Service accounts should not be used for general purpose computing.

Network

A network is a group of interconnected devices that exchange data. Network is a superset of network infrastructure and network architecture.

- **Network Infrastructure:** The collection of network resources that provide connectivity, management, business operations, and communication. It consists of hardware and software, systems and devices, and it enables computing and communication between users, services, applications, and processes. Network infrastructure can be in the cloud, physical, or virtual.

- **Network Architecture:** Refers to how a network is designed, both physically and logically. It defines how a network is organized, including the connections between devices and software as well as the data that is transmitted between them. This should include network architecture diagrams and security architecture diagrams.

Documentation

Policies, processes, procedures, plans, diagrams, and other written material (e.g., compliance reports) either physical or digital. Examples include methods of governance for an enterprise, processes that users follow, or describe network architecture.

- **Plan:** A plan implements policies and may include groups of policies, processes, and procedures.
- **Policy:** A policy is an official governance statement that outlines specific objectives of an information security program.
- **Process:** A set of general tasks and activities to achieve a series of security-related goals.
- **Procedure:** A procedure is an ordered set of steps that must be followed to accomplish a specific task. It provides the approved way of performing an action in a specific technological and organizational environment.

CIS Critical Security Controls

CONTROL 1

Inventory and Control of Enterprise Assets

Safeguards: 5	IG1: 2/5	IG2: 4/5	IG3: 5/5

Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Why is this Control critical?

Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to an enterprise's network. Attackers can take advantage of new assets that are installed, yet not securely configured and patched. Internally, unidentified assets can also have weak security configurations that can make them vulnerable to web- or email-based malware; and, adversaries can leverage weak security configurations for traversing the network, once they are inside.

Additional assets that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should be identified and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex, dynamic enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. However, attackers have shown the ability, patience, and willingness to "inventory and control" our enterprise assets at very large scale in order to support their opportunities.

Another challenge is that portable end-user devices will periodically join a network and then disappear, making the inventory of currently available assets very dynamic. Likewise, cloud environments and virtual machines can be difficult to track in asset inventories when they are shut down or paused.

Another benefit of complete enterprise asset management is supporting incident response, both when investigating the origination of network traffic from an asset on the network and when identifying all potentially vulnerable, or impacted, assets of similar type or location during an incident.

Procedures and tools

This CIS Control requires both technical and procedural actions, united in a process that accounts for, and manages the inventory of, enterprise assets and all associated data throughout its life cycle. It also links to business governance through establishing data/asset owners who are responsible for each component of a business process. Enterprises can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Smaller enterprises can leverage security tools already installed on enterprise assets or used on the network to collect this data. This includes doing a discovery scan of the network with a vulnerability scanner; reviewing anti-malware logs, logs from endpoint security portals, network logs from switches, or authentication logs; and managing the results in a spreadsheet or database.

Maintaining a current and accurate view of enterprise assets is an ongoing and dynamic process. Even for enterprises, there is rarely a single source of truth, as enterprise assets are not always provisioned or installed by the IT department. The reality is that a variety of sources need to be "crowd-sourced" to determine a high-confidence count of enterprise assets. Enterprises can actively scan on a regular basis, sending a variety of different packet types to identify assets connected to the network. In addition to asset sources mentioned above for small enterprises, larger enterprises can collect data from cloud portals and logs from enterprise platforms such as: Active Directory (AD), Single Sign-On (SSO), Multi-Factor Authentication (MFA), Virtual Private Network (VPN), Intrusion Detection Systems (IDS) or Deep Packet Inspection (DPI), Mobile Device Management (MDM), and vulnerability scanning tools. Property inventory databases, purchase order tracking, and local inventory lists are other sources of data to determine which devices are connected. There are tools and methods that normalize this data to identify devices that are unique among these sources.

For cloud-specific guidance, refer to the CIS Controls Cloud Companion Guide: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

For tablet and smart phone guidance, refer to the CIS Controls Mobile Companion Guide: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

For IoT guidance, refer to the CIS Controls Internet of Things Companion Guide:
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

For Industrial Control Systems (ICS) guidance, refer to the CIS Controls ICS Implementation Guide:
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

Safeguards

Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Asset Type: Devices	Security Function: Identify	IG1 IG2 IG3

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

Safeguard 1.2: Address Unauthorized Assets

Asset Type: Devices	Security Function: Respond	IG1 IG2 IG3

Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Safeguard 1.3: Utilize an Active Discovery Tool

Asset Type: Devices	Security Function: Detect	IG2 IG3

Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.

Safeguard 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory

Asset Type: Devices	Security Function: Identify		IG2 IG3

Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.

Safeguard 1.5: Use a Passive Asset Discovery Tool

Asset Type: Devices	Security Function: Detect		IG3

Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.

CONTROL 2

Inventory and Control of Software Assets

Safeguards: 7	IG1: 3/7	IG2: 6/7	IG3: 7/7

Overview

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why is this Control critical?

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software. However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Even if a patch is not yet available, a complete software inventory list allows an enterprise to guard against known attacks until the patch is released. Some sophisticated attackers use "zero-day exploits," which take advantage of previously unknown vulnerabilities that have yet to have a patch released from the software vendor. These software design flaws provide zero days for developers to fix these issues before attackers are able to exploit them. Depending on the severity of the exploit, an enterprise can implement temporary mitigation measures to guard against attacks until the patch is released.

Management of software assets is also important to identify unnecessary security risks. An enterprise should review its software inventory to identify any enterprise assets running software that is not needed for business purposes. For example, an enterprise asset may come installed with default software that creates a potential security risk and provides no benefit to the enterprise. It is critical to inventory, understand, assess, and manage all software connected to an enterprise's infrastructure.

Procedures and tools

Allowlisting can be implemented using a combination of commercial allowlisting tools, policies, or application execution tools that come with anti-malware suites and popular operating systems. Commercial software inventory tools are widely available and used in many enterprises today. The best of these tools provides an inventory check of hundreds of common software used in enterprises. The tools pull information about the patch level of each installed program to ensure that it is the latest version and leverage standardized application names, such as those found in the Common Platform Enumeration (CPE) specification.

Features that implement allowlists are included in many modern endpoint security suites and even natively implemented in certain versions of major operating systems. Moreover, commercial solutions are increasingly bundling together anti-malware, anti-spyware, personal firewall, and host-based IDS and Intrusion Prevention System (IPS), along with application allow and block listing. In particular, most endpoint security solutions can look at the name, file system location, and/or cryptographic hash of a given executable to determine whether the application should be allowed to run on the protected machine. The most effective of these tools offer custom allowlists based on executable path, hash, or regular expression matching. Some even include a non-malicious, yet unapproved, applications function that allows administrators to define rules for execution of specific software for certain users and at certain times of the day.

For cloud-specific guidance, refer to the CIS Controls Cloud Companion Guide:
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

For tablet and smart phone guidance, refer to the CIS Controls Mobile Companion Guide:
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

For IoT guidance, refer to the CIS Controls Internet of Things Companion Guide:
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

For Industrial Control Systems (ICS) guidance, refer to the CIS Controls ICS Implementation Guide:
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

Safeguards

Safeguard 2.1: Establish and Maintain a Software Inventory

Asset Type: Software	Security Function: Identify	IG1 IG2 IG3

Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.

Safeguard 2.2: Ensure Authorized Software is Currently Supported

Asset Type: Software	Security Function: Identify	IG1 IG2 IG3

Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

Safeguard 2.3: Address Unauthorized Software

Asset Type: Software	Security Function: Respond	IG1 IG2 IG3

Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

Safeguard 2.4: Utilize Automated Software Inventory Tools

Asset Type: Software	Security Function: Detect	IG2 IG3

Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

Safeguard 2.5: Allowlist Authorized Software

Asset Type: Software	Security Function: Protect		IG2 IG3

Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

Safeguard 2.6: Allowlist Authorized Libraries

Asset Type: Software	Security Function: Protect		IG2 IG3

Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

Safeguard 2.7: Allowlist Authorized Scripts

Asset Type: Software	Security Function: Protect		IG3

Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, and .py files are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

CONTROL 3
Data Protection

Safeguards: 14	IG1: 6/14	IG2: 12/14	IG3: 14/14

Overview

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Why is this Control critical?

Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Once attackers have penetrated an enterprise's infrastructure, one of their first tasks is to find and exfiltrate data. Enterprises might not be aware that sensitive data is leaving their environment because they are not monitoring data outflows.

While many attacks occur on the network, others involve physical theft of portable end-user devices, attacks on service providers or other partners holding sensitive data. Other sensitive enterprise assets may also include non-computing devices that provide management and control of physical systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

The enterprise's loss of control over protected or sensitive data is a serious and often reportable business impact. While some data is compromised or lost as a result of theft or espionage, the vast majority are a result of poorly understood data management rules, and user error. The adoption of data encryption, both in transit and at rest, can provide mitigation against data compromise, and, even more important, it is a regulatory requirement for most controlled data.

Procedures and tools

It is important for an enterprise to develop a data management process that includes a data management framework, data classification guidelines, and requirements for protection, handling, retention, and disposal of data. There should also be a data breach process that plugs into the incident response plan, and the compliance and communication plans. To derive data sensitivity levels, enterprises need to catalog their key types of data and the overall criticality (impact to its loss or corruption) to the enterprise. This analysis would be used to create an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels.

Once the sensitivity of the data has been defined, a data inventory or mapping should be developed that identifies software accessing data at various sensitivity levels and the enterprise assets that house those applications. Ideally, the network would be separated so that enterprise assets of the same sensitivity level are on the same network and separated from enterprise assets with different sensitivity levels. If possible, firewalls need to control access to each segment, and have user access rules applied to only allow those with a business need to access the data.

For more comprehensive treatment of this topic, we suggest the following resources to help the enterprise with data protection:

NIST® SP 800-88r1 Guides for Media Sanitization: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

---

NIST® FIPS 140-2: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

---

NIST® FIPS 140-3: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

---

For cloud-specific guidance, refer to the CIS Controls Cloud Companion Guide**:**
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

For tablet and smart phone guidance, refer to the CIS Controls Mobile Companion Guide**:**
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

Safeguards

Safeguard 3.1: Establish and Maintain a Data Management Process

Asset Type: Data	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.2: Establish and Maintain a Data Inventory

Asset Type: Data	Security Function: Identify	IG1 IG2 IG3

Establish and maintain a data inventory based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

Safeguard 3.3: Configure Data Access Control Lists

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

Safeguard 3.4: Enforce Data Retention

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.

Safeguard 3.5: Securely Dispose of Data

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

Safeguard 3.6: Encrypt Data on End-User Devices

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

Safeguard 3.7: Establish and Maintain a Data Classification Scheme

Asset Type: Data	Security Function: Identify	IG2 IG3

Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.8: Document Data Flows

Asset Type: Data	Security Function: Identify	IG2 IG3

Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.9: Encrypt Data on Removable Media

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt data on removable media.

Safeguard 3.10: Encrypt Sensitive Data in Transit

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

Safeguard 3.11: Encrypt Sensitive Data at Rest

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

Safeguard 3.12: Segment Data Processing and Storage Based on Sensitivity

Asset Type: Data	Security Function: Protect	IG2 IG3

Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

Safeguard 3.13: Deploy a Data Loss Prevention Solution

Asset Type: Data	Security Function: Protect	IG3

Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's data inventory.

Safeguard 3.14: Log Sensitive Data Access

Asset Type: Data	Security Function: Detect	IG3

Log sensitive data access, including modification and disposal.

CONTROL 4

Secure Configuration of Enterprise Assets and Software

Safeguards: 12	IG1: 7/12	IG2: 11/12	IG3: 12/12

Overview

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Why is this Control critical?

As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared toward ease-of-deployment and ease-of-use rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Service providers play a key role in modern infrastructures, especially for smaller enterprises. They often are not set up by default in the most secure configuration to provide flexibility for their customers to apply their own security policies. Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations. These could introduce weaknesses that are under the responsibility of the enterprise that is using the software, rather than the service provider. This extends to ongoing management and updates, as some Platform as a Service (PaaS) only extend to the operating system, so patching and updating hosted applications are under the responsibility of the enterprise.

Even after a strong initial configuration is developed and applied, it must be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are “tweaked,” to allow the installation of new software or to support new operational requirements.

Procedures and tools

There are many available security baselines for each system. Enterprises should start with these publicly developed, vetted, and supported security benchmarks, security guides, or checklists. Some resources include:

The CIS Benchmarks® Program: http://www.cisecurity.org/cis-benchmarks/

The National Institute of Standards and Technology (NIST®) National Checklist Program Repository: https://nvd.nist.gov/ncp/repository

Enterprises should augment or adjust these baselines to satisfy enterprise security policies, and industry and government regulatory requirements. Deviations of standard configurations and rationale should be documented to facilitate future reviews or audits.

For a larger or more complex enterprise, there will be multiple security baseline configurations based on security requirements or classification of the data on the enterprise asset. Here is an example of the steps to build a secure baseline image:

1. Determine the risk classification of the data handled/stored on the enterprise asset (e.g., high, moderate, low risk).
2. Create a security configuration script that sets system security settings to meet the requirements to protect the data used on the enterprise asset. Use benchmarks, such as the ones described earlier in this section.
3. Install the base operating system software.
4. Apply appropriate operating system and security patches.
5. Install appropriate application software packages, tool, and utilities.
6. Apply appropriate updates to software installed in Step 4.
7. Install local customization scripts to this image.
8. Run the security script created in Step 2 to set the appropriate security level.
9. Run a tool to record/score the system setting of the baseline image.
10. Perform a security quality assurance test.
11. Save this base image in a secure location.

Commercial and/or free configuration management tools, such as the CIS Configuration Assessment Tool (CIS-CAT®) https://learn.cisecurity.org/cis-cat-lite, can be deployed to measure the settings of operating systems and applications of managed machines to look for deviations from the standard image configurations. Commercial configuration management tools use some combination of an agent installed on each managed system, or agentless inspection of systems through remotely logging into each enterprise asset using administrator credentials. Additionally, a hybrid approach is sometimes used whereby a remote session is initiated, a temporary or dynamic agent is deployed on the target system for the scan, and then the agent is removed.

Safeguards

Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets

Asset Type: Devices	Security Function: Protect		IG1 IG2 IG3

Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

Safeguard 4.4: Implement and Manage a Firewall on Servers

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

Safeguard 4.5: Implement and Manage a Firewall on End-User Devices

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Safeguard 4.6: Securely Manage Enterprise Assets and Software

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

Safeguard 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

Asset Type: Devices	Security Function: Protect	IG2 IG3

Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Safeguard 4.9: Configure Trusted DNS Servers on Enterprise Assets

Asset Type: Devices	Security Function: Protect	IG2 IG3

Configure trusted DNS servers on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

Safeguard 4.10: Enforce Automatic Device Lockout on Portable End-User Devices

Asset Type: Devices	Security Function: Protect	IG2 IG3

Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.

Safeguard 4.11: Enforce Remote Wipe Capability on Portable End-User Devices

Asset Type: Data	Security Function: Protect	IG2 IG3

Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Safeguard 4.12: Separate Enterprise Workspaces on Mobile End-User Devices

Asset Type: Data	Security Function: Protect	IG3

Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

CONTROL 5

Account Management

Safeguards: 6	IG1: 4/6	IG2: 6/6	IG3: 6/6

Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Why is this Control critical?

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), social engineering a user to give their password, or using malware to capture passwords or tokens in memory or over the network.

Administrative, or highly privileged, accounts are a particular target, because they allow attackers to add other accounts, or make changes to assets that could make them more vulnerable to other attacks. Service accounts are also sensitive, as they are often shared among teams, internal and external to the enterprise, and sometimes not known about, only to be revealed in standard account management audits.

Finally, account logging and monitoring is a critical component of security operations. While account logging and monitoring are covered in CIS Control 8 (Audit Log Management), it is important in the development of a comprehensive Identity and Access Management (IAM) program.

Procedures and tools

Accounts must be tracked; any account that is dormant must be disabled and eventually removed from the system. There should be periodic audits to ensure all active accounts are traced back to authorized users of the enterprise asset. Look for new accounts added since previous review, especially administrator and service accounts. Close attention should be made to identify and track administrative, or high-privileged accounts and service accounts.

Users with administrator or other privileged access should have separate accounts for those higher authority tasks. These accounts would only be used when performing those tasks or accessing especially sensitive data, to reduce risk in case their normal user account is compromised. For users with multiple accounts, their base user account, used day-to-day for non-administrative tasks, should not have any elevated privileges.

Single Sign-On (SSO) is convenient and secure when an enterprise has many applications, including cloud applications, which helps reduce the number of passwords a user must manage. Users are recommended to use password manager applications to securely store their passwords, and should be instructed not to keep them in spreadsheets or text files on their computers. MFA is recommended for remote access.

Users must also be automatically logged out of the system after a period of inactivity, and be trained to lock their screen when they leave their device to minimize the possibility of someone else in physical proximity around the user accessing their system, applications, or data.

An excellent resource is the NIST® Digital Identity Guidelines: https://pages.nist.gov/800-63-3/

For guidance on the creation and use of passwords, reference the CIS Password Policy Guide: https://www.cisecurity.org/white-papers/cis-password-policy-guide

---

Safeguards

Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Asset Type: Users	Security Function: Identify	IG1 IG2 IG3

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator, and service accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Safeguard 5.2: Use Unique Passwords

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

Safeguard 5.3: Disable Dormant Accounts

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts

Asset Type: Users	Security Function: Identify	IG2 IG3

Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Safeguard 5.6: Centralize Account Management

Asset Type: Users	Security Function: Govern	IG2 IG3

Centralize account management through a directory or identity service.

CONTROL 6

Access Control Management

Safeguards: 8	IG1: 5/8	IG2: 7/8	IG3: 8/8

Overview

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Why is this Control critical?

Where CIS Control 5 deals specifically with account management, CIS Control 6 focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role, and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Accounts should only have the minimal authorization needed for the role. Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

There are some user activities that pose greater risk to an enterprise, either because they are accessed from untrusted networks, or performing administrator functions that allow the ability to add, change, or remove other accounts, or make configuration changes to operating systems or applications to make them less secure. This also enforces the importance of using MFA and Privileged Access Management (PAM) tools.

Some users have access to enterprise assets or data they do not need for their role; this might be due to an immature process that gives all users all access, or lingering access as users change roles within the enterprise over time. Local administrator privileges to users' laptops is also an issue, as any malicious code installed or downloaded by the user can have greater impact on the enterprise asset running as administrator. User, administrator, and service account access should be based on enterprise role and need.

Procedures and tools

There should be a process where privileges are granted and revoked for user accounts. This ideally is based on enterprise role and need through role-based access. Role-based access is a technique to define and manage access requirements for each account based on: need to know, least privilege, privacy requirements, and/or separation of duties. There are technology tools to help manage this process. However, there might be more granular or temporary access based on circumstance.

MFA should be universal for all privileged or administrator accounts. There are many tools that have smartphone applications to perform this function, and are easy to deploy. Using the number-generator feature is more secure than just sending a Short Messaging Service (SMS) message with a one-time code, or prompting a "push" alert for a user to accept. However, neither is recommended for privileged account MFA. PAM tools are available for privileged account control, and provide a one-time password that must be checked out for each use. For additional security in system administration, using "jump-boxes" or out of band terminal connections is recommended.

Comprehensive account de-provisioning is important. Many enterprises have repeatable consistent processes for removing access when employees leave the enterprise. However, that process is not always consistent for contractors, and must be included in the standard de-provisioning process. Enterprises should also inventory and track service accounts, as a common error is leaving clear text tokens or passwords in code, and posting to public cloud-based code repositories.

High-privileged accounts should not be used for day-to-day use, such as web surfing and email reading. Administrators should have separate accounts that do not have elevated privileges for daily office use, and should log into administrator accounts only when performing administrator functions requiring that level of authorization. Security personnel should periodically gather a list of running processes to determine whether any browsers or email readers are running with high privileges.

An excellent resource is the NIST® Digital Identity Guidelines: https://pages.nist.gov/800-63-3/

Safeguards

Safeguard 6.1: Establish an Access Granting Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.

Safeguard 6.2: Establish an Access Revoking Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

Safeguard 6.3: Require MFA for Externally-Exposed Applications

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

Safeguard 6.4: Require MFA for Remote Network Access

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require MFA for remote network access.

Safeguard 6.5: Require MFA for Administrative Access

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

Asset Type: Software	Security Function: Identify		IG2 IG3

Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

Safeguard 6.7: Centralize Access Control

Asset Type: Users	Security Function: Protect		IG2 IG3

Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

Safeguard 6.8: Define and Maintain Role-Based Access Control

Asset Type: Users	Security Function: Govern		IG3

Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

CONTROL 7

Continuous Vulnerability Management

Safeguards: 7	IG1: 4/7	IG2: 7/7	IG3: 7/7

Overview

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Why is this Control critical?

Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate. While there is a gap in time from a vulnerability being known to when it is patched, defenders can prioritize which vulnerabilities are most impactful to the enterprise, or likely to be exploited first due to ease of use. For example, when researchers or the community report new vulnerabilities, vendors have to develop and deploy patches, indicators of compromise (IOCs), and updates. Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches, and install the patch.

There is never perfection in this process. Attackers might be using an exploit to a vulnerability that is not known within the security community. They might have developed an exploit to this vulnerability referred to as a "zero-day" exploit. Once the vulnerability is known in the community, the process mentioned above starts. Therefore, defenders must keep in mind that an exploit might already exist when the vulnerability is widely socialized. Sometimes vulnerabilities might be known within a closed community (e.g., vendor still developing a fix) for weeks, months, or years before it is disclosed publicly. Defenders have to be aware that there might always be vulnerabilities they cannot remediate, and therefore need to use other controls to mitigate.

Enterprises that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their enterprise assets compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, while not impacting the enterprise's business or mission.

Procedures and tools

A large number of vulnerability scanning tools are available to evaluate the security configuration of enterprise assets. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities across an enterprise, it is preferable to use vulnerability scanning tools that map vulnerabilities to one or more of the following industry-recognized vulnerability, configuration, and platform classification schemes and languages: Common Vulnerabilities and Exposures (CVE®), Common Configuration Enumeration (CCE), Open Vulnerability and Assessment Language (OVAL®), Common Platform Enumeration (CPE), Common Vulnerability Scoring System (CVSS), and/or Extensible Configuration Checklist Description Format (XCCDF).

More information on SCAP can be found here: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

---

The frequency of scanning activities should increase as the diversity of an enterprise's assets increases to account for the varying patch cycles of each vendor. Advanced vulnerability scanning tools can be configured with user credentials to authenticate into enterprise assets and perform more comprehensive assessments. These are called "authenticated scans."

In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of enterprise assets. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses from administrators.

Effective enterprises link their vulnerability scanners with problem-ticketing systems that track and report progress on fixing vulnerabilities. This can help highlight unmitigated critical vulnerabilities to senior management to ensure they are resolved. Enterprises can also track how long it took to remediate a vulnerability, after identified, or a patch has been issued. These can support internal or industry compliance requirements. Some mature enterprises will go over these reports in IT security steering committee meetings, which bring leaders from IT and the business together to prioritize remediation efforts based on business impact.

In selecting which vulnerabilities to fix, or patches to apply, an enterprise should augment Forum of Incident Response and Security Teams, Inc.'s (FIRST) Common Vulnerability Scoring System (CVSS) with data concerning the likelihood of a threat actor using a vulnerability, or potential impact of an exploit to the enterprise. Information on the likelihood of exploitation should also be periodically updated based on the most current threat information. For example, the release of a new exploit, or new intelligence relating to exploitation of the vulnerability, should change the priority through which the vulnerability should be considered for patching. Various commercial systems are available to allow an enterprise to automate and maintain this process in a scalable manner.

The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month.

Finally, there should be a quality assurance process to verify configuration updates, or that patches are implemented correctly and across all relevant enterprise assets.

Safeguards

Safeguard 7.1: Establish and Maintain a Vulnerability Management Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 7.2: Establish and Maintain a Remediation Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

Safeguard 7.3: Perform Automated Operating System Patch Management

Asset Type: Software	Security Function: Protect	IG1 IG2 IG3

Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

Safeguard 7.4: Perform Automated Application Patch Management

Asset Type: Software	Security Function: Protect	IG1 IG2 IG3

Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets

Asset Type: Software	Security Function: Identify	IG2 IG3

Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.

Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets

Asset Type: Software	Security Function: Identify	IG2 IG3

Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.

Safeguard 7.7: Remediate Detected Vulnerabilities

Asset Type: Software	Security Function: Respond	IG2 IG3

Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

CONTROL 8

Audit Log Management

Safeguards: 12 | IG1: 3/12 | IG2: 11/12 | IG3: 12/12

Overview

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Why is this Control critical?

Log collection and analysis is critical for an enterprise's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyze them. Attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing.

There are two types of logs that are generally treated and often configured independently: system logs and audit logs. System logs typically provide system-level events that show various system process start/end times, crashes, etc. These are native to systems, and take less configuration to turn on. Audit logs typically include user-level events—when a user logged in, accessed a file, etc.—and take more planning and effort to set up.

Logging records are also critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack. Complete logging records can show, for example, when and how the attack occurred, what information was accessed, and if data was exfiltrated. Retention of logs is also critical in case a follow-up investigation is required or if an attack remained undetected for a long period of time.

Procedures and tools

Most enterprise assets and software offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (Virtual Private Network (VPN), dial-up, etc.) should all be configured for verbose logging where beneficial. Retention of logging data is also important in the event an incident investigation is required.

Furthermore, all enterprise assets should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an enterprise should periodically scan through its logs and compare them with the enterprise asset inventory assembled as part of CIS Control 1, in order to ensure that each managed asset actively connected to the network is periodically generating logs.

Safeguards

Safeguard 8.1: Establish and Maintain an Audit Log Management Process

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

Establish and maintain a documented audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 8.2: Collect Audit Logs

Asset Type: Data	Security Function: Detect		IG1 IG2 IG3

Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

Safeguard 8.3: Ensure Adequate Audit Log Storage

Asset Type: Data	Security Function: Protect		IG1 IG2 IG3

Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

Safeguard 8.4: Standardize Time Synchronization

Asset Type: Network	Security Function: Protect		IG2 IG3

Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.

Safeguard 8.5: Collect Detailed Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Safeguard 8.6: Collect DNS Query Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Collect DNS query audit logs on enterprise assets, where appropriate and supported.

Safeguard 8.7: Collect URL Request Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Collect URL request audit logs on enterprise assets, where appropriate and supported.

Safeguard 8.8: Collect Command-Line Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.

Safeguard 8.9: Centralize Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process. Example implementations primarily include leveraging a SIEM tool to centralize multiple log sources.

Safeguard 8.10: Retain Audit Logs

Asset Type: Data	Security Function: Protect	IG2 IG3

Retain audit logs across enterprise assets for a minimum of 90 days.

Safeguard 8.11: Conduct Audit Log Reviews

Asset Type: Data	Security Function: Detect	IG2 IG3

Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

Safeguard 8.12: Collect Service Provider Logs

Asset Type: Data	Security Function: Detect	IG3

Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

CONTROL 9

Email and Web Browser Protections

Safeguards: 7	IG1: 2/7	IG2: 6/7	IG3: 7/7

Overview

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Why is this Control critical?

Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data, or providing an open channel to allow attackers to gain access, thus increasing risk to the enterprise. Since email and web are the main means that users interact with external and untrusted users and environments, these are prime targets for both malicious code and social engineering. Additionally, as enterprises move to web-based email, or mobile email access, users no longer use traditional full-featured email clients, which provide embedded security controls like connection encryption, strong authentication, and phishing reporting buttons.

Procedures and tools

Web Browser

Cybercriminals can exploit web browsers in multiple ways. If they have access to exploits of vulnerable browsers, they can craft malicious webpages that can exploit those vulnerabilities when browsed with an insecure, or unpatched, browser. Alternatively, they can try to target any number of common web browser third-party plugins that may allow them to hook into the browser or even directly into the operating system or application. These plugins, much like any other software within an environment, need to be reviewed for vulnerabilities, kept up-to-date with latest patches or versions, and controlled. Many come from untrusted sources, and some are even written to be malicious. Therefore, it is best to prevent users from intentionally or unintentionally installing malware that might be hiding in some of these plugins, extensions, and add-ons. Simple configuration updates to the browser can make it much harder for malware to get installed through reducing the ability of installing add-ons/plugins/extensions and preventing specific types of content from automatically executing.

Most popular browsers employ a database of phishing and/or malware sites to protect against the most common threats. A best practice is to enable these content filters and turn on the pop-up blockers. Pop-ups are not only annoying; they can also host embedded malware directly or lure users into clicking links using social engineering tricks. To help enforce blocking of known malicious domains, also consider subscribing to DNS filtering services to block attempts to access these websites at the network level.

Email

Email represents one the most interactive ways humans work with enterprise assets; training and encouraging the right behavior is just as important as the technical settings. Email is the most common threat vector against enterprises through tactics such as phishing and Business Email Compromise (BEC).

Using a spam-filtering tool and malware scanning at the email gateway reduces the number of malicious emails and attachments that come into the enterprise's network. Initiating Domain-based Message Authentication, Reporting, and Conformance (DMARC) helps reduce spam and phishing activities. Installing an encryption tool to secure email and communications adds another layer of user and network-based security. In addition to blocking based on the sender, it is also worthwhile to only allow certain file types that users need for their jobs. This will require coordination with different business units to understand what types of files they receive via email to ensure that there is not an interruption to their processes.

Since phishing email techniques are ever evolving to get past spam filter rules, it is important to train users on how to identify phishing, and to notify IT Security when they see one. There are many platforms that perform phishing tests against users to help educate them on different examples, and track their improvement over time. Crowd-sourcing this knowledge into notifying IT Security teams of phishing helps improve the protections and detections of email-based threats.

Safeguards

Safeguard 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients

Asset Type: Software	Security Function: Protect	IG1 IG2 IG3

Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

Safeguard 9.2: Use DNS Filtering Services

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.

Safeguard 9.3: Maintain and Enforce Network-Based URL Filters

Asset Type: Network	Security Function: Protect	IG2 IG3

Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

Safeguard 9.4: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

Asset Type: Software	Security Function: Protect	IG2 IG3

Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

Safeguard 9.5: Implement DMARC

Asset Type: Network	Security Function: Protect	IG2 IG3

To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

Safeguard 9.6: Block Unnecessary File Types

Asset Type: Network	Security Function: Protect	IG2 IG3

Block unnecessary file types attempting to enter the enterprise's email gateway.

Safeguard 9.7: Deploy and Maintain Email Server Anti-Malware Protections

Asset Type: Network	Security Function: Protect	IG3

Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.

CONTROL 10

Malware Defenses

Safeguards: 7	IG1: 3/7	IG2: 7/7	IG3: 7/7

Overview

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Why is this Control critical?

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques.

Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, and removable media. Malware often relies on insecure end-user behavior, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives. Modern malware is designed to avoid, deceive, or disable defenses.

Malware defenses must be able to operate in this dynamic environment through automation, timely and rapid updating, and integration with other processes like vulnerability management and incident response. They must be deployed at all possible entry points and enterprise assets to detect, prevent spread, or control the execution of malicious software or code.

Procedures and tools

Effective malware protection includes traditional endpoint malware prevention and detection suites. To ensure malware IOCs are up-to-date, enterprises can receive automated updates from the vendor to enrich other vulnerability or threat data. These tools are best managed centrally to provide consistency across the infrastructure.

Being able to block or identify malware is only part of this CIS Control; there is also a focus on centrally collecting the logs to support alerting, identification, and incident response. As malicious actors continue to develop their methodologies, many taking a "living-off-the-land" (LotL) approach to minimize the likelihood of being caught. This approach refers to attacker behavior that uses tools or features that already exist in the target environment. Enabling logging, as per the Safeguards in CIS Control 8, will make it significantly easier for the enterprise to follow the events to understand what happened and why it happened.

CIS provides a series of guides to understand how the CIS Controls apply to the most common living-off-the-land techniques:
https://www.cisecurity.org/controls/resources?crc=minimize-your-threats

---

Safeguards

Safeguard 10.1: Deploy and Maintain Anti-Malware Software

Asset Type: Devices	Security Function: Detect	IG1 IG2 IG3

Deploy and maintain anti-malware software on all enterprise assets.

Safeguard 10.2: Configure Automatic Anti-Malware Signature Updates

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Configure automatic updates for anti-malware signature files on all enterprise assets.

Safeguard 10.3: Disable Autorun and Autoplay for Removable Media

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Disable autorun and autoplay auto-execute functionality for removable media.

Safeguard 10.4: Configure Automatic Anti-Malware Scanning of Removable Media

Asset Type: Devices	Security Function: Detect	IG2 IG3

Configure anti-malware software to automatically scan removable media.

Safeguard 10.5: Enable Anti-Exploitation Features

Asset Type: Devices	Security Function: Protect	IG2 IG3

Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

Safeguard 10.6: Centrally Manage Anti-Malware Software

Asset Type: Devices	Security Function: Protect	IG2 IG3

Centrally manage anti-malware software.

Safeguard 10.7: Use Behavior-Based Anti-Malware Software

Asset Type: Devices	Security Function: Detect	IG2 IG3

Use behavior-based anti-malware software.

CONTROL 11

Data Recovery

Safeguards: 5 | IG1: 4/5 | IG2: 5/5 | IG3: 5/5

Overview

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Why is this Control critical?

In the cybersecurity triad—Confidentiality, Integrity, and Availability (CIA)—the availability of data is, in some cases, more critical than its confidentiality. Enterprises need many types of data to make business decisions, and when that data is not available or is untrusted, then it could impact the enterprise. An easy example is weather information to a transportation enterprise.

When attackers compromise assets, they make changes to configurations, add accounts, and often add software or scripts. These changes are not always easy to identify, as attackers might have corrupted or replaced trusted applications with malicious versions, or the changes might appear to be standard-looking account names. Configuration changes can include adding or changing registry entries, opening ports, turning off security services, deleting logs, or other malicious actions that make a system insecure. These actions do not have to be malicious; human error can cause each of these as well. Therefore, it is important to have an ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state.

There has been an exponential rise in ransomware over the last few years. It is not a new threat, though it has become more commercialized and organized as a reliable method for attackers to make money. If an attacker encrypts an enterprise's data and demands ransom for its restoration, having a recent backup to recover to a known, trusted state can be helpful. However, as ransomware has evolved, it has also become an extortion technique, where data is exfiltrated before being encrypted, and the attacker asks for payment to restore the enterprise's data, as well as to keep it from being sold or publicized. In this case, restoration would only solve the issue of restoring systems to a trusted state and continuing operations. Leveraging the guidance within the CIS Controls will help reduce the risk of ransomware through improved cyber hygiene, as attackers usually use older or basic exploits on insecure systems.

Procedures and tools

Data recovery procedures should be defined in the data management process described in CIS Control 3, Data Protection. This should include backup procedures based on data value, sensitivity, or retention requirements. This will assist in developing backup frequency and type (full vs. incremental).

Once per quarter (or whenever a new backup process or technology is introduced), a testing team should evaluate a random sampling of backups and attempt to restore them on a test bed environment. The restored backups should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

Safeguards

Safeguard 11.1: Establish and Maintain a Data Recovery Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented data recovery process that includes detailed backup procedures. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 11.2: Perform Automated Backups

Asset Type: Data	Security Function: Recover	IG1 IG2 IG3

Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

Safeguard 11.3: Protect Recovery Data

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

Safeguard 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Asset Type: Data	Security Function: Recover		IG1 IG2 IG3

Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

Safeguard 11.5: Test Data Recovery

Asset Type: Data	Security Function: Recover		IG2 IG3

Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

CONTROL 12

Network Infrastructure Management

Safeguards: 8	IG1: 1/8	IG2: 7/8	IG3: 8/8

Overview

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Why is this Control critical?

Secure network infrastructure is an essential defense against attacks. This includes an appropriate security architecture, addressing vulnerabilities that are, often times, introduced with default settings, monitoring for changes, and reassessment of current configurations. Network infrastructure includes devices such as physical and virtualized gateways, firewalls, wireless access points, routers, and switches.

Default configurations for network devices are geared for ease-of-deployment and ease-of-use—not security. Potential default vulnerabilities include open services and ports, default accounts and passwords (including service accounts), support for older vulnerable protocols, and pre-installation of unneeded software. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept data while in transmission.

Network security is a constantly changing environment that necessitates regular re-evaluation of architecture diagrams, configurations, access controls, and allowed traffic flows. Attackers take advantage of network device configurations becoming less secure over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed, but not removed when they are no longer applicable to the business's needs. In some cases, the security risk of an exception is neither properly analyzed nor measured against the associated business need and can change over time.

Procedures and tools

Enterprises should ensure network infrastructure is fully documented and architecture diagrams are kept up-to-date. It is important for key infrastructure components to have vendor support for patches and feature upgrades. Upgrade End-of-Life (EOL) components before the date they will be out of support or apply mitigating controls to isolate them. Enterprises need to monitor their infrastructure versions and configurations for vulnerabilities that would require them to upgrade the network devices to the latest secure and stable version that does not impact the infrastructure.

An up-to-date network architecture diagram, including security architecture diagrams, are an important foundation for infrastructure management. Next is having complete account management for access control, logging, and monitoring. Finally, infrastructure administration should only be performed over secure protocols, with strong authentication (MFA for PAM), and from dedicated administrative devices or out-of-band networks.

Commercial tools can be helpful to evaluate the rule sets of network filtering devices to determine whether they are consistent or in conflict. This provides an automated sanity check of network filters. These tools search for errors in rule sets or Access Controls Lists (ACLs) that may allow unintended services through the network device. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.

For telework and small office guidance, refer to the CIS Controls Telework and Small Office Network Security Guide:
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

Safeguards

Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date

Asset Type: Network	Security Function: Protect	IG1 IG2 IG3

Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network as a service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

Safeguard 12.2: Establish and Maintain a Secure Network Architecture

Asset Type: Network	Security Function: Protect	IG2 IG3

Design and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Example implementations may include documentation, policy, and design components.

Safeguard 12.3: Securely Manage Network Infrastructure

Asset Type: Network	Security Function: Protect	IG2 IG3

Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.

Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 12.5: Centralize Network Authentication, Authorization, and Auditing (AAA)

Asset Type: Network	Security Function: Protect	IG2 IG3

Centralize network AAA.

Safeguard 12.6: Use of Secure Network Management and Communication Protocols

Asset Type: Network	Security Function: Protect	IG2 IG3

Adopt secure network management protocols (e.g., 802.1X) and secure communication protocols (e.g., Wi-Fi Protected Access 2 (WPA2) Enterprise or more secure alternatives).

Safeguard 12.7: Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure

Asset Type: Devices	Security Function: Protect		IG2 IG3

Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

Safeguard 12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work

Asset Type: Devices	Security Function: Protect		IG3

Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

CONTROL 13

Network Monitoring and Defense

Safeguards: 11	IG1: 0/11	IG2: 6/11	IG3: 11/11

Overview

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Why is this Control critical?

We cannot rely on network defenses to be perfect. Adversaries continue to evolve and mature, as they share, or sell, information among their community on exploits and bypasses to security controls. Even if security tools work "as advertised," it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective. Often, misconfigurations due to human error or lack of knowledge of tool capabilities give enterprises a false sense of security.

Security tools can only be effective if they are supporting a process of continuous monitoring that allows staff the ability to be alerted and respond to security incidents quickly. Enterprises that adopt a purely technology-driven approach will also experience more false positives, due to their over-reliance on alerts from tools. Identifying and responding to these threats requires visibility into all threat vectors of the infrastructure and leveraging humans in the process of detection, analysis, and response. It is critical for large or heavily targeted enterprises to have a security operations capability to prevent, detect, and quickly respond to cyber threats before they can impact the enterprise. This process will generate activity reports and metrics that will help enhance security policies, and support regulatory compliance for many enterprises.

As we have seen many times in the press, enterprises have been compromised for weeks, months, or years before discovery. The primary benefit of having comprehensive situational awareness is to increase the speed of detection and response. This is critical to respond quickly when malware is discovered, credentials are stolen, or when sensitive data is compromised to reduce impact to the enterprise.

Through good situational awareness (i.e., security operations), enterprises will identify and catalog Tactics, Techniques, and Procedures (TTPs) of attackers, including their IOCs that will help the enterprise become more proactive in identifying future threats or incidents. Recovery can be achieved faster when the response has access to complete information about the environment and enterprise structure to develop efficient response strategies.

Procedures and tools

Most enterprises do not need to stand up a Security Operations Center (SOC) to gain situational awareness. This starts with first understanding critical business functions, network and server architectures, data and data flows, vendor service and business partner connection, and end-user devices and accounts. This informs the development of a security architecture, technical controls, logging, monitoring, and response procedures.

At the core of this process is a trained and organized team that implements processes for incident detection, analysis, and mitigation. These capabilities could be conducted internally, or through consultants or a managed service provider. Enterprises should consider network, enterprise asset, user credential, and data access activities. Technology will play a crucial role to collect and analyze all of the data, and monitor networks and enterprise assets internally and externally to the enterprise. Enterprises should include visibility to cloud platforms that might not be in line with on-premises security technology.

Forwarding all important logs to analytical programs, such as Security Information and Event Management (SIEM) solutions, can provide value; however, they do not provide a complete picture. Weekly log reviews are necessary to tune thresholds and identify abnormal events. Correlation tools can make audit logs more useful for subsequent manual inspection. These tools are not a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

As this process matures, enterprises will create, maintain, and evolve a knowledge base that will help to understand and assess the business risks, developing an internal threat intelligence capability. Threat intelligence is the collection of TTPs from incidents and adversaries. To accomplish this, a situational awareness program will define and evaluate which information sources are relevant to detect, report, and handle attacks. Most mature enterprises can evolve to threat hunting, where trained staff manually review system and user logs, data flows, and traffic patterns to find anomalies.

Safeguards

Safeguard 13.1: Centralize Security Event Alerting

Asset Type: Network	Security Function: Detect		IG2 IG3

Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

Safeguard 13.2: Deploy a Host-Based Intrusion Detection Solution

Asset Type: Devices	Security Function: Detect		IG2 IG3

Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Safeguard 13.3: Deploy a Network Intrusion Detection Solution

Asset Type: Network	Security Function: Detect		IG2 IG3

Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

Safeguard 13.4: Perform Traffic Filtering Between Network Segments

Asset Type: Network	Security Function: Protect		IG2 IG3

Perform traffic filtering between network segments, where appropriate.

Safeguard 13.5: Manage Access Control for Remote Assets

Asset Type: Devices	Security Function: Protect		IG2 IG3

Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

Safeguard 13.6: Collect Network Traffic Flow Logs

Asset Type: Network	Security Function: Detect		IG2 IG3

Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

Safeguard 13.7: Deploy a Host-Based Intrusion Prevention Solution

Asset Type: Devices	Security Function: Protect	IG3

Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

Safeguard 13.8: Deploy a Network Intrusion Prevention Solution

Asset Type: Network	Security Function: Protect	IG3

Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

Safeguard 13.9: Deploy Port-Level Access Control

Asset Type: Network	Security Function: Protect	IG3

Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

Safeguard 13.10: Perform Application Layer Filtering

Asset Type: Network	Security Function: Protect	IG3

Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

Safeguard 13.11: Tune Security Event Alerting Thresholds

Asset Type: Network	Security Function: Detect	IG3

Tune security event alerting thresholds monthly, or more frequently.

CONTROL 14

Security Awareness and Skills Training

Safeguards: 9	IG1: 8/9	IG2: 9/9	IG3: 9/9

Overview

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Why is this Control critical?

The actions of people play a critical part in the success or failure of an enterprise's security program. It is easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise, than to find a network exploit to do it directly.

Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public sites.

No security program can effectively address cyber risk without a means to address this fundamental human vulnerability. Users at every level of the enterprise have different risks. For example: executives manage more sensitive data; system administrators have the ability to control access to systems and applications; and users in finance, human resources, and contracts all have access to different types of sensitive data that can make them targets.

The training should be updated regularly. This will increase the culture of security and discourage risky workarounds.

Procedures and tools

An effective security awareness training program should not just be a canned, once-a-year training video coupled with regular phishing testing. While annual training is needed, there should also be more frequent, topical messages and notifications about security. This might include messages about: strong password-use that coincides with a media report of password dump, the rise of phishing during tax time, or increased awareness of malicious package delivery emails during the holidays.

Training should also consider the enterprise's different regulatory and threat posture. Financial firms might have more compliance-related training on data handling and use, healthcare enterprises on handling healthcare data, and merchants for credit card data.

Social engineering training, such as phishing tests, should also include awareness of tactics that target different roles. For example, the financial team will receive BEC attempts posing as executives asking to wire money, or receive emails from compromised partners or vendors asking to change the bank account information for their next payment.

For more comprehensive treatment of this topic, the following resources are helpful to build an effective security awareness program:

NIST® SP 800-50 Infosec Awareness Training:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf

---

National Cyber Security Centre (UK): https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

---

EDUCAUSE: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

---

National Cyber Security Alliance (NCSA): https://staysafeonline.org/

SANS: https://www.sans.org/security-awareness-training/resources

---

For guidance on configuring home routers see the CIS Controls Telework and Small Office Network Security Guide**:**
https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

---

Safeguards

Safeguard 14.1: Establish and Maintain a Security Awareness Program

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.

Safeguard 14.3: Train Workforce Members on Authentication Best Practices

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

Safeguard 14.4: Train Workforce on Data Handling Best Practices

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

Safeguard 14.5: Train Workforce Members on Causes of Unintentional Data Exposure

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

Safeguard 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members to be able to recognize a potential incident and be able to report such an incident.

Safeguard 14.7: Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

Safeguard 14.8: Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

Safeguard 14.9: Conduct Role-Specific Security Awareness and Skills Training

Asset Type: Users	Security Function: Protect		IG2 IG3

Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

CONTROL 15

Service Provider Management

Safeguards: 7	IG1: 1/7	IG2: 4/7	IG3: 7/7

Overview

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Why is this Control critical?

In our modern, connected world, enterprises rely on vendors and partners to help manage their data or rely on infrastructure for core applications or functions.

There have been numerous examples where third-party breaches have significantly impacted an enterprise; for example, as early as the late 2000s, payment cards were compromised after attackers infiltrated smaller service providers in the retail industry. More recent examples include ransomware attacks that impact an enterprise indirectly, due to one of their service providers being locked down, causing disruption to business. Or worse, if directly connected, a ransomware attack could encrypt data on the main enterprise.

Most data security and privacy regulations require their protection extend to service providers, such as with Health Insurance Portability and Accountability Act (HIPAA) Business Associate agreements in healthcare, Federal Financial Institutions Examination Council (FFIEC) requirements for the financial industry, and the United Kingdom (U.K.) Cyber Essentials. Third-party trust is a core Governance Risk and Compliance (GRC) function, as risks that are not managed within the enterprise are transferred to entities outside the enterprise.

While reviewing the security of third-parties has been a task performed for decades, there is not a universal standard for assessing security; and, many service providers are being audited by their customers multiple times a month, causing impacts to their own productivity. This is because every enterprise has a different "checklist" or set of standards to grade the service provider. There are only a few industry standards, such as in finance, with the Shared Assessments program, or in higher education, with their Higher Education Community Vendor Assessment Toolkit (HECVAT). Insurance companies selling cybersecurity policies also have their own measurements.

While an enterprise might put a lot of scrutiny into large cloud or application hosting companies because they are hosting their email or critical business applications, smaller firms are often a greater risk. Often times, a service provider contracts with additional parties to provide other plugins or services, such as when a third-party uses a fourth-party platform or product to support the main enterprise.

Procedures and tools

Most enterprises have traditionally used standard checklists, such as ones from ISO 27001 or the CIS Controls. Often, this process is managed through spreadsheets; however, there are online platforms now that allow central management of this process. The focus of this CIS Control though is not on the checklist; instead it is on the fundamentals of the program. Make sure to revisit annually, as relationships and data may change.

No matter what the enterprise's size, there should be a policy about reviewing service providers, an inventory of these vendors, and a risk rating associated with their potential impact to the business in case of an incident. There should also be language in the contracts to hold them accountable if there is an incident that impacts the enterprise.

There are third-party assessment platforms that have an inventory of thousands of service providers, which attempt to provide a central view of the industry, to help enterprises make more informed risk decisions. These platforms often have a dynamic risk score for service providers, based (usually) on passive technical assessments, or enriched through other firms' third-party assessments.

When performing reviews, focus on the services or departments of the provider that are supporting the enterprise. A service provider that has a managed security service contract, or retainer, and holds cybersecurity insurance, can also help with risk reduction.

It is also important to securely decommission service providers when contracts are completed or terminated. Decommission activities may include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

NIST® 800-88r1: Guidelines for Media Sanitization, as appropriate: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

---

Safeguards

Safeguard 15.1: Establish and Maintain an Inventory of Service Providers

Asset Type: Users	Security Function: Identify	IG1 IG2 IG3

Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.3: Classify Service Providers

Asset Type: Users	Security Function: Govern	IG2 IG3

Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.4: Ensure Service Provider Contracts Include Security Requirements

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

Safeguard 15.5: Assess Service Providers

Asset Type: Users	Security Function: Govern		IG3

Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.

Safeguard 15.6: Monitor Service Providers

Asset Type: Data	Security Function: Govern		IG3

Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

Safeguard 15.7: Securely Decommission Service Providers

Asset Type: Data	Security Function: Protect		IG3

Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

CONTROL 16

Application Software Security

Safeguards: 14 | **IG1:** 0/14 | **IG2:** 11/14 | **IG3:** 14/14

Overview

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Why is this Control critical?

Applications provide a human-friendly interface to allow users to access and manage data in a way that is aligned to business functions. They also minimize the need for users to deal directly with complex (and potentially error-prone) system functions, like logging into a database to insert or modify files. Enterprises use applications to manage their most sensitive data and control access to system resources. Therefore, an attacker can use the application itself to compromise the data, instead of an elaborate network and system hacking sequence that attempts to bypass network security controls and sensors. This is why protecting user credentials (specifically application credentials) defined in CIS Control 6 is so important.

Lacking credentials, application flaws are the attack vector of choice. However, today's applications are developed, operated, and maintained in a highly complex, diverse, and dynamic environment. Applications run on multiple platforms: web, mobile, cloud, etc., with application architectures that are more complex than legacy client-server or database-web server structures. Development life cycles have become shorter, transitioning from months or years in long waterfall methodologies, to DevOps cycles with frequent code updates. Also, applications are rarely created from scratch, and are often "assembled" from a complex mix of development frameworks, libraries, existing code, and new code. There are also modern and evolving data protection regulations dealing with user privacy. These may require compliance to regional or sector-specific data protection requirements.

These factors make traditional approaches to security, like control (of processes, code sources, run-time environment, etc.), inspection, and testing, much more challenging. Also, the risk that an application vulnerability introduces might not be understood, except in a specific operational setting or context.

Application vulnerabilities can be present for many reasons: insecure design, insecure infrastructure, coding mistakes, weak authentication, and failure to test for unusual or unexpected conditions. Attackers can exploit specific vulnerabilities, including buffer overflows, exposure to Structured Query Language (SQL) injection, cross-site scripting, cross-site request forgery, and click-jacking of code to gain access to sensitive data, or take control over vulnerable assets within the infrastructure as a launching point for further attacks.

Applications and websites can also be used to harvest credentials, data, or attempt to install malware onto the users who access them.

Finally, it is now more common to acquire Software as a Service (SaaS) platforms, where software is developed and managed entirely through a third-party. These might be hosted anywhere in the world. This brings challenges to enterprises that need to know what risks they are accepting with using these platforms; and, they often do not have visibility into the development and application security practices of these platforms. Some of these SaaS platforms allow for customizing of their interfaces and databases. Enterprises that extend these applications should follow this CIS Control, similar to if they were doing ground-up customer development.

Procedures and tools

For Version 8, CIS partnered with SAFECode to help develop the procedures and Safeguards for this updated Application Software Security Control. However, application software security is a large topic on its own, and so (consistent with the principles of the overall CIS Controls), we focus here on the most critical Safeguards. These were derived from a companion paper on application software security that SAFECode developed (referenced below), which provides a more in-depth treatment of the topic, and is consistent with SAFECode's existing body of content.

SAFECode developed a three-tiered approach to help readers identify which Development Group (DG) they fit in as a maturity scale for development programs. The three CIS IG levels used within the Safeguards inspired their approach for the DGs below:

Development Group 1

The enterprise largely relies on off-the-shelf or Open Source Software (OSS) and packages with only the occasional addition of small applications or website coding. The enterprise is capable of applying basic operational and procedural best practices and of managing the security of its vendor-supplied software as a result of following the guidance of the CIS Controls.

Development Group 2

The enterprise relies on some custom (in-house or contractor-developed) web and/or native code applications integrated with third-party components and runs on-premises or in the cloud. The enterprise has a development staff that applies software development best practices. The enterprise is attentive to the quality and maintenance of third-party open source or commercial code on which it depends.

Development Group 3

The enterprise makes a major investment in custom software that it requires to run its business and serve its customers. It may host software on its own infrastructure, in the cloud, or both, and may integrate a large range of third-party open source and commercial software components. Software vendors and enterprises that deliver SaaS should consider Development Group 3 as a minimum set of requirements.

The first step in developing an application security program is implementing a vulnerability management process. This process must integrate into the development life cycle, and should be lightweight to insert into the standard bug-fixing progress. The process should include root cause analysis to fix underlying flaws so as to reduce future vulnerabilities, and a severity rating to prioritize remediation efforts.

Developers need to be trained in application security concepts and secure coding practices. This includes a process to acquire or evaluate third-party software, modules, and libraries used in the application to ensure they do not introduce security flaws. The developers should be taught what types of modules they can securely use, where they can be safely acquired, and which components they can, or should not, develop themselves (e.g., encryption).

Weaknesses in the infrastructure that supports these applications can introduce risk. The CIS Controls and the concept of minimizing the attack surface can help secure networks, systems, and accounts that are used within the application. Specific guidance can be found in CIS Controls 1-7, 12, and 13.

The ideal application security program is one that introduces security as early into the software development life cycle as possible. The management of security problems should be consistent and integrated with standard software flaw/bug management, as opposed to a separate process that competes for development resources. Larger or more mature development teams should consider the practice of threat modeling in the design phase. Design-level vulnerabilities are less common than code-level vulnerabilities; however, they often are very severe and much harder to fix quickly. Threat modeling is the process of identifying and addressing application security design flaws before code is created. Threat modeling requires specific training, technical, and business knowledge. It is best conducted through internal "security champions" in each development team, to lead threat modeling practices for that team's software. It also provides valuable context to downstream activities, such as root cause analysis and security testing.

Larger, or commercial, development teams may also consider a bug bounty program where individuals are paid for finding flaws in their applications. Such a program is best used to supplement an in-house secure development process and can provide an efficient mechanism for identifying classes of vulnerabilities that the process needs to focus on.

Finally, in 2020 NIST® published its Secure Software Development Framework (SSDF), which brought together what the industry has learned about software security over the past two decades and created a secure software development framework for planning, evaluating, and communicating about software security activities. Enterprises acquiring software or services can use this framework to build their security requirements and understand whether a software provider's development process follows best practices. These are some application security resources:

SAFECode Application Security Addendum: https://safecode.org/cis-controls/

NIST® SSDF: https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf

The Software Alliance: https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

OWASP®: https://owasp.org/

Safeguards

Safeguard 16.1: Establish and Maintain a Secure Application Development Process

Asset Type: Documentation	Security Function: Govern		IG2 IG3

Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Asset Type: Documentation	Security Function: Govern		IG2 IG3

Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

Safeguard 16.3: Perform Root Cause Analysis on Security Vulnerabilities

Asset Type: Software	Security Function: Detect		IG2 IG3

Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

Safeguard 16.4: Establish and Manage an Inventory of Third-Party Software Components

Asset Type: Software	Security Function: Identify	IG2 IG3

Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

Safeguard 16.5: Use Up-to-Date and Trusted Third-Party Software Components

Asset Type: Software	Security Function: Protect	IG2 IG3

Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

Safeguard 16.6: Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

Safeguard 16.7: Use Standard Hardening Configuration Templates for Application Infrastructure

Asset Type: Software	Security Function: Protect	IG2 IG3

Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

Safeguard 16.8: Separate Production and Non-Production Systems

Asset Type: Network	Security Function: Protect	IG2 IG3

Maintain separate environments for production and non-production systems.

Safeguard 16.9: Train Developers in Application Security Concepts and Secure Coding

Asset Type: Users	Security Function: Protect	IG2 IG3

Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

Safeguard 16.10: Apply Secure Design Principles in Application Architectures

Asset Type: Software	Security Function: Protect	IG2 IG3

Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

Safeguard 16.11: Leverage Vetted Modules or Services for Application Security Components

Asset Type: Software	Security Function: Protect	IG2 IG3

Leverage vetted modules or services for application security components, such as identity management, encryption, auditing, and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

Safeguard 16.12: Implement Code-Level Security Checks

Asset Type: Software	Security Function: Protect	IG3

Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

Safeguard 16.13: Conduct Application Penetration Testing

Asset Type: Software	Security Function: Detect	IG3

Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

Safeguard 16.14: Conduct Threat Modeling

Asset Type: Software	Security Function: Protect	IG3

Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

CONTROL 17

Incident Response Management

Safeguards: 9	IG1: 3/9	IG2: 8/9	IG3: 9/9

Overview

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Why is this Control critical?

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to original state, and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

We cannot expect our protections to be effective 100% of the time. When an incident occurs, if an enterprise does not have a documented plan—even with good people—it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

Along with detection, containment, and eradication, communication to stakeholders is key. If we are to reduce the probability of material impact due to a cyber event, the enterprise's leadership must know what potential impact there could be, so that they can help prioritize remediation or restoration decisions that best support the enterprise. These business decisions could be based on regulatory compliance, disclosure rules, service-level agreements with partners or customers, revenue, or mission impacts.

Dwell time from when an attack happens to when it is identified can be days, weeks, or months. The longer the attacker is in the enterprise's infrastructure, the more embedded they become and they will develop more ways to maintain persistent access for when they are eventually discovered. With the rise of ransomware, which is a stable moneymaker for attackers, this dwell time is critical, especially with modern tactics of stealing data before encrypting it for ransom.

Procedures and tools

Even if an enterprise does not have resources to conduct incident response within an enterprise, it is still critical to have a documented plan. This would include the sources for protections and detections, a list of who to call upon for assistance, and communication plans about how to convey information to leadership, employees, regulators, partners, and customers.

After defining incident response procedures, the incident response team, or a third-party, should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and potential impacts the enterprise faces. These scenarios help ensure that enterprise leadership and technical team members understand their role in the incident response process to help prepare them to handle incidents. It is inevitable that exercise and training scenarios will identify gaps in plans and processes, and unexpected dependencies, which can then be updated into the plan.

More mature enterprises should include threat intelligence and/or threat hunting into their incident response process. This will help the team become more proactive, identifying key or primary attackers to their enterprise or industry to monitor or search for their TTPs. This will help focus detections and define response procedures to identify and remediate more quickly.

The actions in CIS Control 17 provide specific, high-priority steps that can improve enterprise security, and should be a part of any comprehensive incident response plan. In addition, we recommend the following resource dedicated to this topic:

Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide:
CREST provides guidance, standards, and knowledge on a wide variety of cyber defense topics.
https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf

---

Safeguards

Safeguard 17.1: Designate Personnel to Manage Incident Handling

Asset Type: Users	Security Function: Respond	IG1 IG2 IG3

Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.2: Establish and Maintain Contact Information for Reporting Security Incidents

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service providers, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

Safeguard 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

Establish and maintain an documented enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.4: Establish and Maintain an Incident Response Process

Asset Type: Documentation	Security Function: Govern		IG2 IG3

Establish and maintain a documented incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.5: Assign Key Roles and Responsibilities

Asset Type: Users	Security Function: Respond		IG2 IG3

Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, analysts, and relevant third parties. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.6: Define Mechanisms for Communicating During Incident Response

Asset Type: Users	Security Function: Respond		IG2 IG3

Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, secure chat, or notification letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.7: Conduct Routine Incident Response Exercises

Asset Type: Users	Security Function: Recover		IG2 IG3

Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

Safeguard 17.8: Conduct Post-Incident Reviews

Asset Type: Users	Security Function: Recover		IG2 IG3

Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Safeguard 17.9: Establish and Maintain Security Incident Thresholds

Asset Type: Documentation	Security Function: Recover		IG3

Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

CONTROL 18

Penetration Testing

Safeguards: 5	IG1: 0/5	IG2: 3/5	IG3: 5/5

Overview

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Why is this Control critical?

A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, combined with appropriate action from people. However, it is rarely perfect. In a complex environment where technology is constantly evolving and new attacker tradecraft appears regularly, enterprises should periodically test their controls to identify gaps and to assess their resiliency. This test may be from external network, internal network, application, system, or device perspective. It may include social engineering of users, or physical access control bypasses.

Often, penetration tests are performed for specific purposes:

- As a “dramatic” demonstration of an attack, usually to convince decision-makers of their enterprise’s weaknesses
- As a means to test the correct operation of enterprise defenses (“verification”)
- To test that the enterprise has built the right defenses in the first place (“validation”)

Independent penetration testing can provide valuable and objective insights about the existence of vulnerabilities in enterprise assets and humans, and the efficacy of defenses and mitigating controls to protect against adverse impacts to the enterprise. They are part of a comprehensive, ongoing program of security management and improvement. They can also reveal process weaknesses, such as incomplete or inconsistent configuration management, or end-user training.

Penetration testing differs from vulnerability testing, described in CIS Control 7. Vulnerability testing just checks for presence of known, insecure enterprise assets, and stops there. Penetration testing goes further to exploit those weaknesses to see how far an attacker could get, and what business process or data might be impacted through exploitation of that vulnerability. This is an important detail, and often penetration testing and vulnerability testing are incorrectly used interchangeably. Vulnerability testing is exclusively automated scanning with sometimes manual validation of false positives, whereas penetration testing requires more human involvement and analysis, sometimes supported through the use of custom tools or scripts. However, vulnerability testing is often a starting point for a penetration test.

Another common term is "Red Team" exercises. These are similar to penetration tests in that vulnerabilities are exploited; however, the difference is the focus. Red Teams simulate specific attacker TTPs to evaluate how an enterprise's environment would withstand an attack from a specific adversary, or category of adversaries.

Procedures and tools

Penetration testing starts with the reconnaissance of the enterprise and environment, and scanning to identify the vulnerabilities that can be used as entries into the enterprise. It is important to make sure all enterprise assets are discovered that are in-scope, and not just rely on a static list, which might be outdated or incomplete. Next, vulnerabilities will be identified in these targets. Exploits to these vulnerabilities are executed to demonstrate specifically how an adversary can either subvert the enterprise's security goals (e.g., the protection of specific sensitive data) or achieve specific adversarial objectives (e.g., the establishment of a covert Command and Control (C2) infrastructure). The results provide deeper insight, through demonstration, into the business risks of various vulnerabilities. This can be against physical access controls, network, system, or application layers, and often includes social engineering components.

Penetration tests are expensive, complex, and potentially introduce their own risks. Experienced people from reputable vendors must conduct them. Some risks include unexpected shutdown of systems that might be unstable, exploits that might delete or corrupt data or configurations, and the output of a testing report that needs to be protected itself, because it gives step-by-step instructions on how to break into the enterprise to target critical assets or data.

Each enterprise should define a clear scope and rules of engagement for penetration testing. The scope of such projects should include, at a minimum, enterprise assets with the highest valued information and production processing functionality. Other lower-value systems may also be tested to see if they can be used as pivot points to compromise higher-value targets. The rules of engagement for penetration test analyses should describe, at a minimum, times of day for testing, duration of test(s), and the overall test approach. Only a few people in the enterprise should know when a penetration test is performed, and a primary point of contact in the enterprise should be designated if problems occur. Increasingly popular recently is having penetration tests conducted through third-party legal counsel to protect the penetration test report from disclosure.

The Safeguards in this CIS Control provide specific, high-priority steps that can improve enterprise security, and should be a part of any penetration testing. In addition, we recommend the use of some of the excellent comprehensive resources dedicated to this topic to support security test planning, management, and reporting:

OWASP Penetration Testing Methodologies: https://www.owasp.org/index.php/Penetration_testing_methodologies

PCI Security Standards Council: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Safeguards

Safeguard 18.1: Establish and Maintain a Penetration Testing Program

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

Safeguard 18.2: Perform Periodic External Penetration Tests

Asset Type: Network	Security Function: Detect	IG2 IG3

Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

Safeguard 18.3: Remediate Penetration Test Findings

Asset Type: Network	Security Function: Protect	IG2 IG3

Remediate penetration test findings based on the enterprise's documented vulnerability remediation process. This should include determining a timeline and level of effort based on the impact and prioritization of each identified finding.

Safeguard 18.4: Validate Security Measures

Asset Type: Network	Security Function: Protect	IG3

Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.

Safeguard 18.5: Perform Periodic Internal Penetration Tests

Asset Type: Network	Security Function: Detect	IG3

Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

Appendix

Acronyms and Abbreviations

AAA	Authentication, Authorization, and Auditing
ACL	Access Control List
AD	Active Directory
AoC	Attestation of Compliance
API	Application Programming Interface
BEC	Business Email Compromise
C2	Command and Control
CCE	Common Configuration Enumeration
CDM	Community Defense Model
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CIS-CAT	CIS Configuration Assessment Tool
COTS	Commercial off-the-Shelf
CPE	Common Platform Enumeration
CREST	Council of Registered Security Testers
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DBIR	Data Breach Investigations Report
DEP	Data Execution Prevention
DG	Development Group
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMS	Database Management System
DNS	Domain Name System
DPI	Deep Packet Inspection
EDR	Endpoint Detection and Response
EOL	End of Life
FFIEC	Federal Financial Institutions Examination Council
FIRST	Forum of Incident Response and Security Teams, Inc.
FISMA	Federal Information Security Modernization Act
GRC	Governance Risk and Compliance
HECVAT	Higher Education Community Vendor Assessment Toolkit
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
IDS	Intrusion Detection System
IG	Implementation Group
IOCs	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization

IT	Information Technology
LotL	Living off the Land
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge®
MS-ISAC	Multi-State Information Sharing and Analysis Center
NaaS	Network as a Service
NCSA	National Cyber Security Alliance
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OS	Operating System
OSS	Open Source Software
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI	Payment Card Industry
SaaS	Software as a Service
SAFECode	Software Assurance Forum for Excellence in Code
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SIP	System Integrity Protection
SMS	Short Messaging Service
SOC	Security Operations Center
SOC 2	Service Organization Control 2
SPF	Sender Policy Framework
SQL	Structured Query Language
SSDF	Secure Software Development Framework
SSH	Secure Shell
SSO	Single Sign-On
Telnet	Teletype Network
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
U.K.	United Kingdom
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access 2
XCCDF	Extensible Configuration Checklist Description Format

Change Log

Two minor releases (v8.1.1 – August 2024 and v8.1.2 – March 2025) have resulted in the following changes:

- Correction of some minor typos in our **Asset Class section (pg. 8)** and **Glossary (Appendix A3)**
- Update of hyperlinks throughout the document, based on the recent release of the **CIS Controls Resources webpage**
- Correction of two Security Function typos – Safeguards 16.11 (Protect) and 16.13 (Detect)
- Correction of some minor typos for Safeguards 5.1, 8.9, 11.1, 16.11, and 17.5.

Glossary

Accounts

Accounts are a profile, identity, or membership created for a person, group, or machine entity that grant access to resources or functionalities within a computer system or network. A system of accounts is important for managing permissions and security levels across an enterprise, and an individual may have access to multiple accounts depending on job roles and security requirements. User accounts are for individual users and are tailored for the specific tasks their roles and responsibilities require. User accounts, administrator accounts, and service accounts are subsets of accounts.

Administrator accounts

Accounts for users requiring escalated privileges. The accounts are used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure. Each administrator account should be assigned to a single user. Common administrator account subtypes include root accounts, local administrator, domain administrator accounts, and network or security appliance administrator accounts.

Application Programming Interface (API)

A set of rules and interfaces for software components to interact with each other in a standardized way. APIs allow applications to access and communicate with both internal and external resources.[1]

Applications

A program, or a group of programs, running on top of an operating system hosted on an enterprise asset. Example application types include web, database, cloud-based, and mobile. Applications are considered a software asset in this document.

Asset Class

A group of information assets that are evaluated as one set based on their similarity. Devices, Software, Data, Users, Network, and Documentation are examples.

Authentication systems

A system or mechanism used to identify a user through associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system, user directory service, or within an authentication server. Examples of authentication systems can include active directory, Multi-Factor Authentication (MFA), biometrics, and tokens.

Authorization systems

A system or mechanism used to determine access levels or user/client privileges related to system resources including files, services, computer programs, data, and application features. An authorization system grants or denies access to a resource based on the user's identity. Examples of authorization systems can include active directory, access control lists, and role-based access control lists.

Bi-annually

Every six months. Any tasks that should be done bi-annually should also be repeated whenever significant change has occurred that would affect the network or devices in question, including changes such as hardware upgrades or mergers and acquisitions.

Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses sensitive or confidential information; or an authorized user accesses sensitive or confidential information for other than authorized purposes.

Cloud environment

A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

[1] NIST: https://csrc.nist.gov/glossary/term/application_programming_interface

Data

A collection of facts that can be examined, considered, and used for decision-making. Although data may be physical, the CIS Controls primarily provide protection for digital data that may be stored, transferred, and processed by enterprise assets.

Data Exposure

An unintentional data breach.

Database

Organized collection of data, generally stored and accessed electronically from a computer system. Databases can reside remotely or on-site. Database Management Systems (DMSs) are used to administer databases, and are not considered part of a database for this document.

Devices

Devices are enterprise assets (data processing and storage assets), end-user devices, portable devices, mobile devices, servers, Internet of Things and non-computing devices, network devices, and removable media. Devices may exist in physical spaces, virtual infrastructure, or cloud-based environments. Devices can remotely connect to these systems.

Documentation

Policies, processes, procedures, plans, diagrams, and other written material (e.g., compliance reports) either physical or digital. Examples include methods of governance for an enterprise, processes that users follow, or describe network architecture.

Dwell Time

The period of time between an initial attack and the detection of an intrusion when an attacker has unauthorized access to the data and the environment.

End-user devices

Information technology (IT) assets used among members of an enterprise during work or off-hours. End-user devices include desktops and workstations, as well as portable and mobile devices such as laptops, smartphones, and tablets. For the purpose of this document, end-user devices are a subset of enterprise assets.

Enterprise

An enterprise is any business or organization that uses computer systems, networks, and devices.

Enterprise assets

Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments.

Externally-exposed applications

Refers to applications that are public facing and discoverable through reconnaissance and network scanning from the public internet outside of the enterprise's network.

Externally-exposed enterprise assets

Refers to enterprise assets that are public facing and discoverable through domain name system reconnaissance and network scanning from the public internet outside of the enterprise's network.

Firmware

Software stored within a device's non-volatile memory, such as ROM or flash memory, used to allow different types of hardware to communicate with the operating system. Firmware is often updated outside of the enterprise's operating system and application software update process.

Govern

NIST CSF 2.0 Security Function Govern is defined as the organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The Govern Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.[2]

Internal enterprise assets

Refers to non-public facing enterprise assets that can only be identified through network scans and reconnaissance from within an enterprise's network through authorized authenticated or unauthenticated access.

[2] NIST Reference Format for NIST Publications: https://www.nist.gov/nist-research-library/reference-format-nist-publications

Internet of Things (IoT) and Non-computing Devices

Devices embedded with sensors, software, and other technologies. These devices may connect, store, and exchange data with other devices and systems. The device's connection to the internet can be intermittent, non-existent, or persistent. Examples of these devices include smart watches and other wearables, printers, smart screens, smart home devices, speakers, industrial control systems, and physical security sensors. For the purpose of this document, IoT and non-computing devices are a subset of enterprise assets.

Library

A shareable pre-compiled codebase to include classes, procedures, scripts, configuration data, and more, used to develop software programs and applications. Libraries are designed to assist both the programmer and the programming language compiler in building and executing software more efficiently.

Log Data

A computer-generated data file that records the events occurring within the enterprise. Examples of logs include: operating system, anti-malware detection, database, application, network, firewall, web server, or access control logs (e.g., electronic locks, alarm system).

Mobile devices

Small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. For the purpose of this document, mobile devices are a subset of portable devices.

Multi-factor authentication

Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password), something you have (e.g., cryptographic identification device, token), or something you are (e.g., biometric). [3]

Network

A network is a group of interconnected devices that exchange data. Network is a superset of network infrastructure and network architecture.

Network Architecture

Refers to how a network is designed, both physically and logically. It defines how a network is organized, including the connections between devices and software as well as the data that is transmitted between them. This should include network architecture diagrams and security architecture diagrams.

Network Asset

A group of interconnected devices that exchange data. Enterprises may operate one or more networks that are managed together or independently.

Network Devices

Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware, as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets. Note that network devices are listed under Enterprise Assets because they are managed much like other devices, however, they also play a dual role in the Network Asset Class when related to the communication over a network.

Network Infrastructure

The collection of network resources that provide connectivity, management, business operations, and communication. It consists of hardware and software, systems and devices, and it enables computing and communication between users, services, applications, and processes. Network infrastructure can be in the cloud, physical, or virtual.

Non-computing/Internet of Things (IoT) devices

Devices embedded with sensors, software, and other technologies for the purpose of connecting, storing, and exchanging data with other devices and systems over the internet. While these devices are not used for computational processes, they support an enterprise's ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems, and information technology sensors. For the purpose of this document, non-computing/IoT devices are a subset of enterprise assets.

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Operating system

Software on enterprise assets that manages computer hardware and software resources and provides common services for programs. Example operating systems include Windows, Ubuntu, MacOS, Android, and z/OS. Operating systems are considered a software asset.

Phishing

A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.[4]

Physical data

Data that is stored in physical documents or stored on physical types of removable devices (e.g., USB drives, tape backups). Physical data may be sensitive or not.

Physical environment

Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network.

Plan

A plan implements policies and may include groups of policies, processes, and procedures.

Policy

A policy is an official governance statement that outlines specific objectives of an information security program.

Portable devices

Transportable, end-user devices that have the capability to wirelessly connect to a network. Portable devices can include laptops which may require external hardware for connectivity and mobile devices, such as smartphones and tablets. For the purpose of this document, portable devices are a subset of end-user devices.

Pretexting

Part of a social engineering attack that involves inventing a scenario to convince the victim to divulge information that should not be divulged. The purpose of pretexting is to convince the victim of the legitimacy of the communication. The method of this type of attack can be through any communication method or medium.

Procedure

A procedure is an ordered set of steps that must be followed to accomplish a specific task. It provides the approved way of performing an action in a specific technological and organizational environment.

Process

A set of general tasks and activities to achieve a series of security-related goals.

Remote devices

Any enterprise asset capable of connecting to a network remotely, usually from public internet. This can include enterprise assets such as end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers.

Remote file systems

Enable an application that runs on an enterprise asset to access files stored on a different asset. Remote file systems often make other resources, such as remote non-computing devices, accessible from an asset. The remote file access takes place using some form of local area network, wide area network, point-to-point link, or other communication mechanism. These file systems are often referred to as network file systems or distributed file systems.

Removable media

Any type of storage device that can be removed from a computer while the system is running and allows data to be moved from one system to another. Examples of removable media include CDs, DVDs, Blu-ray Discs, external hard drives, SD cards, tape backups, diskettes, and USB drives.

Script

Uncompiled code that requires a software environment to execute.

Sensitive Data

Physical or digital data stored, processed, or managed by the enterprise that must be kept private, accurate, reliable, and available. If released or destroyed in an unauthorized manner, it would cause harm to the enterprise or its customers. These impacts may be due to a data breach or a violation of a policy, contract, or regulation.

[4] https://tools.ietf.org/html/rfc4949

Servers

A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Servers can exist in datacenters, public/private/hybrid cloud environments, including temporal containers or serverless workloads. Examples of servers include web servers, application servers, mail servers, and file servers. For the purpose of this document, servers are a subset of enterprise assets.

Service accounts

A service account is created specifically to run applications, services, and automated tasks on an operating system. Service accounts may also be created just to own data and configuration files. Each service account should be used for a specific service or function, and it should have an assigned owner who is responsible for how the account is used. Service accounts should not be used for general purpose computing.

Services

Specialized programs that perform well-defined critical tasks for the operating system. Services often start with the operating system, run-in in the background, and can be stopped and started by users. Example services include managing network communications, users, file permissions, system security, and device interaction.

Service Provider

Entity that offers platforms, software, and services to other enterprises. Examples include IT consultants, managed service provider (MSPs), Software as a Service (SaaS) platforms, and cloud service providers. Third-party providers and vendors are also considered Service Providers. These services may be paid or free. Some relationships may or may not require a contract or SLA in place. Examples include data analysis, traffic blocking, and similar services.

Social engineering

Refers to a broad range of malicious activities accomplished through human interactions on various platforms, such as email or phone. It relies on psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Software

Sets of data and instructions used to direct a computer to complete a specific task. Software assets include operating systems and applications. Both may contain services, libraries, or Application Programming Interfaces (APIs).

Tailgating

A physical security issue where an individual follows another into a secured area without properly authenticating or following established protocols for entering the area.

Third-Party Provider

See Service Provider.

Users

Employees, third-party vendors, contractors, service providers, consultants, or any other person who is authorized to access an enterprise asset. This also includes user, administrator, and service accounts.

User accounts

An identity comprised of a set of credentials (e.g., username, password) that defines a user on a computer or computing system. A user account keeps track of a user's information and settings, controls the files, folders, and resources a user is allowed to access, as well as the tasks a user is allowed to perform. For the purpose of this document, user accounts refer to "standard" user accounts with limited privileges and are used for general tasks.

Virtual environment

Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work.

Workforce

All individuals who are employed or engaged by an organization and have access to its information systems, assets, or resources. It includes all employees both on-site and remote, excluding service providers and consultants.

Resources and References

A Roadmap to the CIS Critical Security Controls: https://www.cisecurity.org/insights/white-papers/roadmap-cis-critical-security-controls

CIS Benchmarks®: http://www.cisecurity.org/cis-benchmarks/

CIS Controls Cloud Companion Guide: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-cloud-companion-guide

CIS Controls Mappings: https://www.cisecurity.org/controls/resources?crc=other-security-frameworks

CIS Controls Navigator: https://www.cisecurity.org/controls/cis-controls-navigator

CIS Controls Policy Templates: https://www.cisecurity.org/controls/resources?crc=implementation-tools-guidance

CIS Controls Resources: https://www.cisecurity.org/controls/resources?crc=about-the-cis-critical-security-controls

CIS Community Defense Model (CDM): https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

CIS Configuration Assessment Tool (CIS-CAT®): https://learn.cisecurity.org/cis-cat/

CIS Controls Assessment Specification: https://cas.docs.cisecurity.org/en/latest/

CIS Controls Industrial Control Systems Implementation Guide: https://www.cisecurity.org/insights/white-papers/cis-critical-security-controls-v8-1-industrial-control-systems-ics-guide

CIS Controls Internet of Things Companion Guide: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

CIS Controls Mobile Companion Guide: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

CIS Controls Self Assessment Tool (CSAT): https://www.cisecurity.org/controls/cis-controls-self-assessment-tool-cis-csat/

CIS Controls Telework and Small Office Network Security Guide: https://www.cisecurity.org/controls/resources?crc=environment-specific-guidance

CIS CSAT Ransomware Business Impact Analysis (BIA) Tool: https://www.cisecurity.org/cis-securesuite/business-impact-analysis-tool

CIS WorkBench: https://www.cisecurity.org/insights/blog/how-to-get-up-and-running-with-cis-workbench

CIS Password Policy Guide: https://www.cisecurity.org/white-papers/cis-password-policy-guide

CIS Risk Assessment Method (RAM): https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/

Cost of Cyber Defense for IG1: https://www.cisecurity.org/controls/resources?crc=assess-and-measure

Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide: https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf

EDUCAUSE: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

Establishing Essential Cyber Hygiene (v8.1): https://www.cisecurity.org/insights/white-papers/establishing-essential-cyber-hygiene-version-8-1

Guide to Asset Classes: https://www.cisecurity.org/insights/white-papers/guide-to-asset-classes-cis-critical-security-controls-v8-1

Guide to Implementation Groups (IG) - CIS Critical Security Controls v8.1: https://www.cisecurity.org/insights/white-papers/guide-implementation-groups-ig-cis-critical-security-controls-v8-1

International Organization for Standardization: https://www.iso.org/home.html

National Cyber Security Alliance (NCSA): https://staysafeonline.org/

National Cyber Security Centre (U.K.): https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

National Institute of Standards and Technology (NIST®): https://www.nist.gov/

National Institute of Standards and Technology (NIST®) Cybersecurity Framework (CSF) 2.0: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Institute of Standards and Technology (NIST®) Digital Identity Guidelines: https://pages.nist.gov/800-63-3/

National Institute of Standards and Technology (NIST®) FIPS 140-2: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

National Institute of Standards and Technology (NIST®) FIPS 140-3: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

National Institute of Standards and Technology (NIST®) National Checklist Program Repository: https://nvd.nist.gov/ncp/repository

National Institute of Standards and Technology (NIST®) SP 800-50 Infosec Awareness Training: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf

National Institute of Standards and Technology (NIST®) SP 800-88r1—Guidelines for Media Sanitization: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Institute of Standards and Technology (NIST®) SP 800-126r3 The Technical Specification for the Security Content Automation Protocol (SCAP): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

National Institute of Standards and Technology (NIST®) SSDF: https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf

OWASP®: https://owasp.org/

OWASP® Penetration Testing Methodologies: https://www.owasp.org/index.php/Penetration_testing_methodologies

PCI Security Standards Council: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Privacy Companion Guide for Controls v8: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-privacy-companion-guide

SAFECode Application Security Addendum: https://safecode.org/cis-controls/

SANS: https://www.sans.org/security-awareness-training/resources

SME Guide for Controls v8: https://www.cisecurity.org/insights/white-papers/implementation-guide-for-small-and-medium-sized-enterprises-cis-controls-ig1

The Software Alliance: https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

Trailhead Training Courses for CIS Controls: https://www.cisecurity.org/controls/trailhead-training-courses

Verizon Data Breach Investigations Report:
https://www.verizon.com/business/resources/reports/dbir/

Controls and Safeguards Index

CONTROL 1
Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory

Asset Type: Devices	Security Function: Identify	IG1 IG2 IG3

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.

Safeguard 1.2: Address Unauthorized Assets

Asset Type: Devices	Security Function: Respond	IG1 IG2 IG3

Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

Safeguard 1.3: Utilize an Active Discovery Tool

Asset Type: Devices	Security Function: Detect	IG2 IG3

Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.

Safeguard 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory

Asset Type: Devices	Security Function: Identify	IG2 IG3

Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.

Safeguard 1.5: Use a Passive Asset Discovery Tool

Asset Type: Devices	Security Function: Detect	IG3

Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.

CONTROL 2
Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Safeguard 2.1: Establish and Maintain a Software Inventory

Asset Type: Software	Security Function: Identify	IG1 IG2 IG3

Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.

Safeguard 2.2: Ensure Authorized Software is Currently Supported

Asset Type: Software	Security Function: Identify	IG1 IG2 IG3

Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.

Safeguard 2.3: Address Unauthorized Software

Asset Type: Software	Security Function: Respond	IG1 IG2 IG3

Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

Safeguard 2.4: Utilize Automated Software Inventory Tools

Asset Type: Software	Security Function: Detect	IG2 IG3

Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

Safeguard 2.5: Allowlist Authorized Software

Asset Type: Software	Security Function: Protect	IG2 IG3

Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.

Safeguard 2.6: Allowlist Authorized Libraries

Asset Type: Software	Security Function: Protect	IG2 IG3

Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

Safeguard 2.7: Allowlist Authorized Scripts

Asset Type: Software	Security Function: Protect	IG3

Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1 and .py files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

CONTROL 3
Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Safeguard 3.1: Establish and Maintain a Data Management Process

Asset Type: Data	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.2: Establish and Maintain a Data Inventory

Asset Type: Data	Security Function: Identify	IG1 IG2 IG3

Establish and maintain a data inventory based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

Safeguard 3.3: Configure Data Access Control Lists

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.

Safeguard 3.4: Enforce Data Retention

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.

Safeguard 3.5: Securely Dispose of Data

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.

Safeguard 3.6: Encrypt Data on End-User Devices

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

Safeguard 3.7: Establish and Maintain a Data Classification Scheme

Asset Type: Data	Security Function: Identify	IG2 IG3

Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.8: Document Data Flows

Asset Type: Data	Security Function: Identify	IG2 IG3

Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 3.9: Encrypt Data on Removable Media

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt data on removable media.

Safeguard 3.10: Encrypt Sensitive Data in Transit

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).

Safeguard 3.11: Encrypt Sensitive Data at Rest

Asset Type: Data	Security Function: Protect	IG2 IG3

Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

Safeguard 3.12: Segment Data Processing and Storage Based on Sensitivity

Asset Type: Data	Security Function: Protect	IG2 IG3

Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.

Safeguard 3.13: Deploy a Data Loss Prevention Solution

Asset Type: Data	Security Function: Protect	IG3

Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's data inventory.

Safeguard 3.14: Log Sensitive Data Access

Asset Type: Data	Security Function: Detect	IG3

Log sensitive data access, including modification and disposal.

CONTROL 4
Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Safeguard 4.1: Establish and Maintain a Secure Configuration Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.

Safeguard 4.4: Implement and Manage a Firewall on Servers

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.

Safeguard 4.5: Implement and Manage a Firewall on End-User Devices

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Safeguard 4.6: Securely Manage Enterprise Assets and Software

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.

Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

Safeguard 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

Asset Type: Devices	Security Function: Protect	IG2 IG3

Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.

Safeguard 4.9: Configure Trusted DNS Servers on Enterprise Assets

Asset Type: Devices	Security Function: Protect	IG2 IG3

Configure trusted DNS servers on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

Safeguard 4.10: Enforce Automatic Device Lockout on Portable End-User Devices

Asset Type: Devices	Security Function: Protect	IG2 IG3

Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.

Safeguard 4.11: Enforce Remote Wipe Capability on Portable End-User Devices

Asset Type: Data	Security Function: Protect	IG2 IG3

Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.

Safeguard 4.12: Separate Enterprise Workspaces on Mobile End-User Devices

Asset Type: Data	Security Function: Protect	IG3

Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

CONTROL 5

Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Safeguard 5.1: Establish and Maintain an Inventory of Accounts

Asset Type: Users	Security Function: Identify	IG1 IG2 IG3

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator, and service accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Safeguard 5.2: Use Unique Passwords

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

Safeguard 5.3: Disable Dormant Accounts

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts

Asset Type: Users	Security Function: Identify	IG2 IG3

Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Safeguard 5.6: Centralize Account Management

Asset Type: Users	Security Function: Govern	IG2 IG3

Centralize account management through a directory or identity service.

CONTROL 6
Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Safeguard 6.1: Establish an Access Granting Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.

Safeguard 6.2: Establish an Access Revoking Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

Safeguard 6.3: Require MFA for Externally-Exposed Applications

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

Safeguard 6.4: Require MFA for Remote Network Access

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require MFA for remote network access.

Safeguard 6.5: Require MFA for Administrative Access

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

Safeguard 6.6: Establish and Maintain an Inventory of Authentication and Authorization Systems

Asset Type: Software	Security Function: Identify	IG2 IG3

Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.

Safeguard 6.7: Centralize Access Control

Asset Type: Users	Security Function: Protect	IG2 IG3

Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

Safeguard 6.8: Define and Maintain Role-Based Access Control

Asset Type: Users	Security Function: Govern		IG3

Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

CONTROL 7

Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Safeguard 7.1: Establish and Maintain a Vulnerability Management Process

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 7.2: Establish and Maintain a Remediation Process

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.

Safeguard 7.3: Perform Automated Operating System Patch Management

Asset Type: Software	Security Function: Protect		IG1 IG2 IG3

Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

Safeguard 7.4: Perform Automated Application Patch Management

Asset Type: Software	Security Function: Protect	IG1 IG2 IG3

Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets

Asset Type: Software	Security Function: Identify	IG2 IG3

Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.

Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets

Asset Type: Software	Security Function: Identify	IG2 IG3

Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.

Safeguard 7.7: Remediate Detected Vulnerabilities

Asset Type: Software	Security Function: Respond	IG2 IG3

Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

CONTROL 8

Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Safeguard 8.1: Establish and Maintain an Audit Log Management Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 8.2: Collect Audit Logs

Asset Type: Data	Security Function: Detect	IG1 IG2 IG3

Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

Safeguard 8.3: Ensure Adequate Audit Log Storage

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

Safeguard 8.4: Standardize Time Synchronization

Asset Type: Data	Security Function: Protect	IG2 IG3

Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.

Safeguard 8.5: Collect Detailed Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

Safeguard 8.6: Collect DNS Query Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Collect DNS query audit logs on enterprise assets, where appropriate and supported.

Safeguard 8.7: Collect URL Request Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Collect URL request audit logs on enterprise assets, where appropriate and supported.

Safeguard 8.8: Collect Command-Line Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.

Safeguard 8.9: Centralize Audit Logs

Asset Type: Data	Security Function: Detect	IG2 IG3

Centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process. Example implementations primarily include leveraging a SIEM tool to centralize multiple log sources.

Safeguard 8.10: Retain Audit Logs

Asset Type: Data	Security Function: Protect	IG2 IG3

Retain audit logs across enterprise assets for a minimum of 90 days.

Safeguard 8.11: Conduct Audit Log Reviews

Asset Type: Data	Security Function: Detect	IG2 IG3

Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.

Safeguard 8.12: Collect Service Provider Logs

Asset Type: Data	Security Function: Detect	IG3

Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.

CONTROL 9
Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Safeguard 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients

Asset Type: Software	Security Function: Protect	IG1 IG2 IG3

Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

Safeguard 9.2: Use DNS Filtering Services

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.

Safeguard 9.3: Maintain and Enforce Network-Based URL Filters

Asset Type: Network	Security Function: Protect	IG2 IG3

Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

Safeguard 9.4: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

Asset Type: Software	Security Function: Protect	IG2 IG3

Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

Safeguard 9.5: Implement DMARC

Asset Type: Network	Security Function: Protect	IG2 IG3

To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

Safeguard 9.6: Block Unnecessary File Types

Asset Type: Network	Security Function: Protect	IG2 IG3

Block unnecessary file types attempting to enter the enterprise's email gateway.

Safeguard 9.7: Deploy and Maintain Email Server Anti-Malware Protections

Asset Type: Network	Security Function: Protect	IG3

Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.

CONTROL 10
Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Safeguard 10.1: Deploy and Maintain Anti-Malware Software

Asset Type: Devices	Security Function: Detect	IG1 IG2 IG3

Deploy and maintain anti-malware software on all enterprise assets.

Safeguard 10.2: Configure Automatic Anti-Malware Signature Updates

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Configure automatic updates for anti-malware signature files on all enterprise assets.

Safeguard 10.3: Disable Autorun and Autoplay for Removable Media

Asset Type: Devices	Security Function: Protect	IG1 IG2 IG3

Disable autorun and autoplay auto-execute functionality for removable media.

Safeguard 10.4: Configure Automatic Anti-Malware Scanning of Removable Media

Asset Type: Devices	Security Function: Detect	IG2 IG3

Configure anti-malware software to automatically scan removable media.

Safeguard 10.5: Enable Anti-Exploitation Features

Asset Type: Devices	Security Function: Protect	IG2 IG3

Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

Safeguard 10.6: Centrally Manage Anti-Malware Software

Asset Type: Devices	Security Function: Protect	IG2 IG3

Centrally manage anti-malware software.

Safeguard 10.7: Use Behavior-Based Anti-Malware Software

Asset Type: Devices	Security Function: Detect	IG2 IG3

Use behavior-based anti-malware software.

CONTROL 11
Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Safeguard 11.1: Establish and Maintain a Data Recovery Process

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a documented data recovery process that includes detailed backup procedures. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 11.2: Perform Automated Backups

Asset Type: Data	Security Function: Recover	IG1 IG2 IG3

Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.

Safeguard 11.3: Protect Recovery Data

Asset Type: Data	Security Function: Protect	IG1 IG2 IG3

Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.

Safeguard 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Asset Type: Data	Security Function: Recover	IG1 IG2 IG3

Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.

Safeguard 11.5: Test Data Recovery

Asset Type: Data	Security Function: Recover	IG2 IG3

Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

CONTROL 12
Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date

Asset Type: Network	Security Function: Protect	IG1 IG2 IG3

Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network as a service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.

Safeguard 12.2: Establish and Maintain a Secure Network Architecture

Asset Type: Network	Security Function: Protect	IG2 IG3

Design and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Example implementations may include documentation, policy, and design components.

Safeguard 12.3: Securely Manage Network Infrastructure

Asset Type: Network	Security Function: Protect	IG2 IG3

Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.

Safeguard 12.4: Establish and Maintain Architecture Diagram(s)

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 12.5: Centralize Network Authentication, Authorization, and Auditing (AAA)

Asset Type: Network	Security Function: Protect	IG2 IG3

Centralize network AAA.

Safeguard 12.6: Use of Secure Network Management and Communication Protocols

Asset Type: Network	Security Function: Protect	IG2 IG3

Adopt secure network management protocols (e.g., 802.1X) and secure communication protocols (e.g., Wi-Fi Protected Access 2 (WPA2) Enterprise or more secure alternatives).

Safeguard 12.7: Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure

Asset Type: Devices	Security Function: Protect	IG2 IG3

Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.

Safeguard 12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work

Asset Type: Devices	Security Function: Protect	IG3

Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.

CONTROL 13
Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Safeguard 13.1: Centralize Security Event Alerting

Asset Type: Network	Security Function: Detect	IG2 IG3

Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

Safeguard 13.2: Deploy a Host-Based Intrusion Detection Solution

Asset Type: Devices	Security Function: Detect	IG2 IG3

Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Safeguard 13.3: Deploy a Network Intrusion Detection Solution

Asset Type: Network	Security Function: Detect	IG2 IG3

Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

Safeguard 13.4: Perform Traffic Filtering Between Network Segments

Asset Type: Network	Security Function: Protect	IG2 IG3

Perform traffic filtering between network segments, where appropriate.

Safeguard 13.5: Manage Access Control for Remote Assets

Asset Type: Devices	Security Function: Protect	IG2 IG3

Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

Safeguard 13.6: Collect Network Traffic Flow Logs

Asset Type: Network	Security Function: Detect	IG2 IG3

Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

Safeguard 13.7: Deploy a Host-Based Intrusion Prevention Solution

Asset Type: Devices	Security Function: Protect	IG3

Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

Safeguard 13.8: Deploy a Network Intrusion Prevention Solution

Asset Type: Network	Security Function: Protect	IG3

Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

Safeguard 13.9: Deploy Port-Level Access Control

Asset Type: Network	Security Function: Protect	IG3

Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.

Safeguard 13.10: Perform Application Layer Filtering

Asset Type: Network	Security Function: Protect	IG3

Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

Safeguard 13.11: Tune Security Event Alerting Thresholds

Asset Type: Network	Security Function: Detect	IG3

Tune security event alerting thresholds monthly, or more frequently.

CONTROL 14

Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Safeguard 14.1: Establish and Maintain a Security Awareness Program

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.

Safeguard 14.3: Train Workforce Members on Authentication Best Practices

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

Safeguard 14.4: Train Workforce on Data Handling Best Practices

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

Safeguard 14.5: Train Workforce Members on Causes of Unintentional Data Exposure

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

Safeguard 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members to be able to recognize a potential incident and be able to report such an incident.

Safeguard 14.7: Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

Safeguard 14.8: Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

Asset Type: Users	Security Function: Protect	IG1 IG2 IG3

Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

Safeguard 14.9: Conduct Role-Specific Security Awareness and Skills Training

Asset Type: Users	Security Function: Protect		IG2 IG3

Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

CONTROL 15
Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Safeguard 15.1: Establish and Maintain an Inventory of Service Providers

Asset Type: Users	Security Function: Identify		IG1 IG2 IG3

Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.2: Establish and Maintain a Service Provider Management Policy

Asset Type: Documentation	Security Function: Govern		IG2 IG3

Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.3: Classify Service Providers

Asset Type: Users	Security Function: Govern	IG2 IG3

Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 15.4: Ensure Service Provider Contracts Include Security Requirements

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.

Safeguard 15.5: Assess Service Providers

Asset Type: Users	Security Function: Govern	IG3

Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.

Safeguard 15.6: Monitor Service Providers

Asset Type: Data	Security Function: Govern	IG3

Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

Safeguard 15.7: Securely Decommission Service Providers

Asset Type: Data	Security Function: Protect	IG3

Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

CONTROL 16
Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Safeguard 16.1: Establish and Maintain a Secure Application Development Process

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

Safeguard 16.3: Perform Root Cause Analysis on Security Vulnerabilities

Asset Type: Software	Security Function: Protect	IG2 IG3

Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

Safeguard 16.4: Establish and Manage an Inventory of Third-Party Software Components

Asset Type: Software	Security Function: Identify	IG2 IG3

Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

Safeguard 16.5: Use Up-to-Date and Trusted Third-Party Software Components

Asset Type: Software	Security Function: Protect	IG2 IG3

Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

Safeguard 16.6: Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

Safeguard 16.7: Use Standard Hardening Configuration Templates for Application Infrastructure

Asset Type: Software	Security Function: Protect		IG2 IG3

Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

Safeguard 16.8: Separate Production and Non-Production Systems

Asset Type: Network	Security Function: Protect		IG2 IG3

Maintain separate environments for production and non-production systems.

Safeguard 16.9: Train Developers in Application Security Concepts and Secure Coding

Asset Type: Users	Security Function: Protect		IG2 IG3

Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

Safeguard 16.10: Apply Secure Design Principles in Application Architectures

Asset Type: Software	Security Function: Protect		IG2 IG3

Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

Safeguard 16.11: Leverage Vetted Modules or Services for Application Security Components

Asset Type: Software	Security Function: Protect	IG2 IG3

Leverage vetted modules or services for application security components, such as identity management, encryption, auditing, and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

Safeguard 16.12: Implement Code-Level Security Checks

Asset Type: Software	Security Function: Protect	IG3

Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

Safeguard 16.13: Conduct Application Penetration Testing

Asset Type: Software	Security Function: Detect	IG3

Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

Safeguard 16.14: Conduct Threat Modeling

Asset Type: Software	Security Function: Protect	IG3

Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

CONTROL 17

Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Safeguard 17.1: Designate Personnel to Manage Incident Handling

Asset Type: Users	Security Function: Respond	IG1 IG2 IG3

Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.2: Establish and Maintain Contact Information for Reporting Security Incidents

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service providers, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.

Safeguard 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents

Asset Type: Documentation	Security Function: Govern	IG1 IG2 IG3

Establish and maintain an documented enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.4: Establish and Maintain an Incident Response Process

Asset Type: Documentation	Security Function: Govern		IG2 IG3

Establish and maintain a documented incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.5: Assign Key Roles and Responsibilities

Asset Type: Users	Security Function: Respond		IG2 IG3

Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, analysts, and relevant third parties. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.6: Define Mechanisms for Communicating During Incident Response

Asset Type: Users	Security Function: Respond		IG2 IG3

Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, secure chat, or notification letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Safeguard 17.7: Conduct Routine Incident Response Exercises

Asset Type: Users	Security Function: Recover		IG2 IG3

Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.

Safeguard 17.8: Conduct Post-Incident Reviews

Asset Type: Users	Security Function: Recover	IG2 IG3

Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

Safeguard 17.9: Establish and Maintain Security Incident Thresholds

Asset Type: Documentation	Security Function: Recover	IG3

Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

CONTROL 18
Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Safeguard 18.1: Establish and Maintain a Penetration Testing Program

Asset Type: Documentation	Security Function: Govern	IG2 IG3

Establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

Safeguard 18.2: Perform Periodic External Penetration Tests

Asset Type: Network	Security Function: Detect	IG2 IG3

Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

Safeguard 18.3: Remediate Penetration Test Findings

Asset Type: Network	Security Function: Protect	IG2 IG3

Remediate penetration test findings based on the enterprise's documented vulnerability remediation process. This should include determining a timeline and level of effort based on the impact and prioritization of each identified finding.

Safeguard 18.4: Validate Security Measures

Asset Type: Network	Security Function: Protect	IG3

Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.

Safeguard 18.5: Perform Periodic Internal Penetration Tests

Asset Type: Network	Security Function: Detect	IG3

Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CIS Center for Internet Security®

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security

CenterforIntSec
@CISecurity
TheCISecurity
cisecurity

CIS Controls Implementation

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
1				Inventory and Control of Enterprise Assets	*Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.*			
1	1.1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	x	x	x
1	1.2	Devices	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	x	x	x
1	1.3	Devices	Detect	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.		x	x
1	1.4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.		x	x
1	1.5	Devices	Detect	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.			x
2				Inventory and Control of Software Assets	*Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.*			
2	2.1	Software	Identify	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, decommission date, and number of licenses. Review and update the software inventory bi-annually, or more frequently.	x	x	x
2	2.2	Software	Identify	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	x	x	x
2	2.3	Software	Respond	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	x	x	x
2	2.4	Software	Detect	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.		x	x
2	2.5	Software	Protect	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		x	x
2	2.6	Software	Protect	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, and .so files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		x	x
2	2.7	Software	Protect	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1 and .py files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			x
3				Data Protection	*Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.*			
3	3.1	Data	Govern	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
3	3.2	Data	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	x	x	x
3	3.3	Data	Protect	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	x	x	x
3	3.4	Data	Protect	Enforce Data Retention	Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.	x	x	x
3	3.5	Data	Protect	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	x	x	x
3	3.6	Data	Protect	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	x	x	x
3	3.7	Data	Identify	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x

CIS Controls Implementation

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
3	3.8	Data	Identify	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x
3	3.9	Data	Protect	Encrypt Data on Removable Media	Encrypt data on removable media.		x	x
3	3.10	Data	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		x	x
3	3.11	Data	Protect	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		x	x
3	3.12	Data	Protect	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		x	x
3	3.13	Data	Protect	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's data inventory.			x
3	3.14	Data	Detect	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.			x
4				**Secure Configuration of Enterprise Assets and Software**	***Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).***			
4	4.1	Documentation	Govern	Establish and Maintain a Secure Configuration Process	Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
4	4.2	Documentation	Govern	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
4	4.3	Devices	Protect	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	x	x	x
4	4.4	Devices	Protect	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	x	x	x
4	4.5	Devices	Protect	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	x	x	x
4	4.6	Devices	Protect	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	x	x	x
4	4.7	Users	Protect	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	x	x	x
4	4.8	Devices	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		x	x
4	4.9	Devices	Protect	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on network infrastructure. Example implementations include configuring network devices to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		x	x
4	4.10	Devices	Protect	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		x	x
4	4.11	Data	Protect	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.		x	x
4	4.12	Data	Protect	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.			x
5				**Account Management**	***Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.***			
5	5.1	Users	Identify	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must at a minimum include user, administrator, and service accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	x	x	x
5	5.2	Users	Protect	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.	x	x	x

CIS Controls Implementation

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
5	5.3	Users	Protect	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	x	x	x
5	5.4	Users	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	x	x	x
5	5.5	Users	Identify	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		x	x
5	5.6	Users	Govern	Centralize Account Management	Centralize account management through a directory or identity service.		x	x
6				**Access Control Management**	***Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.***			
6	6.1	Documentation	Govern	Establish an Access Granting Process	Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.	x	x	x
6	6.2	Documentation	Govern	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	x	x	x
6	6.3	Users	Protect	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	x	x	x
6	6.4	Users	Protect	Require MFA for Remote Network Access	Require MFA for remote network access.	x	x	x
6	6.5	Users	Protect	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.	x	x	x
6	6.6	Software	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.		x	x
6	6.7	Users	Protect	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		x	x
6	6.8	Users	Govern	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			x
7				**Continuous Vulnerability Management**	***Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.***			
7	7.1	Documentation	Govern	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
7	7.2	Documentation	Govern	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	x	x	x
7	7.3	Software	Protect	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x
7	7.4	Software	Protect	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	x	x	x
7	7.5	Software	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans.		x	x
7	7.6	Software	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets. Perform scans on a monthly, or more frequent, basis.		x	x
7	7.7	Software	Respond	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		x	x
8				**Audit Log Management**	***Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.***			
8	8.1	Documentation	Govern	Establish and Maintain an Audit Log Management Process	Establish and maintain a documented audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
8	8.2	Data	Detect	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	x	x	x
8	8.3	Data	Protect	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	x	x	x
8	8.4	Network	Protect	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		x	x
8	8.5	Data	Detect	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		x	x
8	8.6	Data	Detect	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.		x	x
8	8.7	Data	Detect	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.		x	x

CIS Controls Implementation

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
8	8.8	Data	Detect	Collect Command-Line Audit Logs	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		x	x
8	8.9	Data	Detect	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process. Example implementations primarily include leveraging a SIEM tool to centralize multiple log sources.		x	x
8	8.10	Data	Protect	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.		x	x
8	8.11	Data	Detect	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		x	x
8	8.12	Data	Detect	Collect Service Provider Logs	Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.			x
9				**Email and Web Browser Protections**	***Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.***			
9	9.1	Software	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	x	x	x
9	9.2	Devices	Protect	Use DNS Filtering Services	Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.	x	x	x
9	9.3	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		x	x
9	9.4	Software	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		x	x
9	9.5	Network	Protect	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		x	x
9	9.6	Network	Protect	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.		x	x
9	9.7	Network	Protect	Deploy and Maintain Email Server Anti-Malware Protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.			x
10				**Malware Defenses**	***Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.***			
10	10.1	Devices	Detect	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.	x	x	x
10	10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.	x	x	x
10	10.3	Devices	Protect	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	x	x	x
10	10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.		x	x
10	10.5	Devices	Protect	Enable Anti-Exploitation Features	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		x	x
10	10.6	Devices	Protect	Centrally Manage Anti-Malware Software	Centrally manage anti-malware software.		x	x
10	10.7	Devices	Detect	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.		x	x
11				**Data Recovery**	***Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.***			
11	11.1	Documentation	Govern	Establish and Maintain a Data Recovery Process	Establish and maintain a documented data recovery process that includes detailed backup procedures. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
11	11.2	Data	Recover	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	x	x	x
11	11.3	Data	Protect	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	x	x	x
11	11.4	Data	Recover	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.	x	x	x
11	11.5	Data	Recover	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.		x	x
12				**Network Infrastructure Management**	***Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.***			
12	12.1	Network	Protect	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network as a service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	x	x	x

CIS Controls Implementation

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
12	12.2	Network	Protect	Establish and Maintain a Secure Network Architecture	Design and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Example implementations may include documentation, policy, and design components.		x	x
12	12.3	Network	Protect	Securely Manage Network Infrastructure	Securely manage network infrastructure. Example implementations include version-controlled Infrastructure-as-Code (IaC), and the use of secure network protocols, such as SSH and HTTPS.		x	x
12	12.4	Documentation	Govern	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x
12	12.5	Network	Protect	Centralize Network Authentication, Authorization, and Auditing (AAA)	Centralize network AAA.		x	x
12	12.6	Network	Protect	Use of Secure Network Management and Communication Protocols	Adopt secure network management protocols (e.g., 802.1X) and secure communication protocols (e.g., Wi-Fi Protected Access 2 (WPA2) Enterprise or more secure alternatives).		x	x
12	12.7	Devices	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		x	x
12	12.8	Devices	Protect	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			x
13				**Network Monitoring and Defense**	***Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.***			
13	13.1	Network	Detect	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		x	x
13	13.2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.		x	x
13	13.3	Network	Detect	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.		x	x
13	13.4	Network	Protect	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.		x	x
13	13.5	Devices	Protect	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		x	x
13	13.6	Network	Detect	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		x	x
13	13.7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.			x
13	13.8	Network	Protect	Deploy a Network Intrusion Prevention Solution	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.			x
13	13.9	Network	Protect	Deploy Port-Level Access Control	Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			x
13	13.10	Network	Protect	Perform Application Layer Filtering	Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			x
13	13.11	Network	Detect	Tune Security Event Alerting Thresholds	Tune security event alerting thresholds monthly, or more frequently.			x
14				**Security Awareness and Skills Training**	***Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.***			
14	14.1	Documentation	Govern	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
14	14.2	Users	Protect	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.	x	x	x
14	14.3	Users	Protect	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	x	x	x
14	14.4	Users	Protect	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	x	x	x
14	14.5	Users	Protect	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	x	x	x

CIS Controls Implementation

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
14	14.6	Users	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.	x	x	x
14	14.7	Users	Protect	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	x	x	x
14	14.8	Users	Protect	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	x	x	x
14	14.9	Users	Protect	Conduct Role-Specific Security Awareness and Skills Training	Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.		x	x
15				**Service Provider Management**	***Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.***			
15	15.1	Users	Identify	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
15	15.2	Documentation	Govern	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x
15	15.3	Users	Govern	Classify Service Providers	Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x
15	15.4	Documentation	Govern	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.		x	x
15	15.5	Users	Govern	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.			x
15	15.6	Data	Govern	Monitor Service Providers	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.			x
15	15.7	Data	Protect	Securely Decommission Service Providers	Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.			x
16				**Application Software Security**	***Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.***			
16	16.1	Documentation	Govern	Establish and Maintain a Secure Application Development Process	Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x
16	16.2	Documentation	Govern	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.		x	x
16	16.3	Software	Detect	Perform Root Cause Analysis on Security Vulnerabilities	Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.		x	x
16	16.4	Software	Identify	Establish and Manage an Inventory of Third-Party Software Components	Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.		x	x

CIS Controls Implementation

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
16	16.5	Software	Protect	Use Up-to-Date and Trusted Third-Party Software Components	Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.		x	x
16	16.6	Documentation	Govern	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.		x	x
16	16.7	Software	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.		x	x
16	16.8	Network	Protect	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.		x	x
16	16.9	Users	Protect	Train Developers in Application Security Concepts and Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.		x	x
16	16.10	Software	Protect	Apply Secure Design Principles in Application Architectures	Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.		x	x
16	16.11	Software	Protect	Leverage Vetted Modules or Services for Application Security Components	Leverage vetted modules or services for application security components, such as identity management, encryption, auditing, and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		x	x
16	16.12	Software	Protect	Implement Code-Level Security Checks	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.			x
16	16.13	Software	Detect	Conduct Application Penetration Testing	Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.			x
16	16.14	Software	Protect	Conduct Threat Modeling	Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.			x
17				**Incident Response Management**	***Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.***			
17	17.1	Users	Respond	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
17	17.2	Documentation	Govern	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service providers, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	x	x	x
17	17.3	Documentation	Govern	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain a documented enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	x	x	x
17	17.4	Documentation	Govern	Establish and Maintain an Incident Response Process	Establish and maintain a documented incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x
17	17.5	Users	Respond	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, analysts, and relevant third parties. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x
17	17.6	Users	Respond	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, secure chat, or notification letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		x	x

CIS Controls Implementation

CIS Control	CIS Safeguard	Asset Class	Security Function	Title	Description	IG1	IG2	IG3
17	17.7	Users	Recover	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.		x	x
17	17.8	Users	Recover	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.		x	x
17	17.9	Documentation	Recover	Establish and Maintain Security Incident Thresholds	Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.			x
18				**Penetration Testing**	***Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.***			
18	18.1	Documentation	Govern	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.		x	x
18	18.2	Network	Detect	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.		x	x
18	18.3	Network	Protect	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's documented vulnerability remediation process. This should include determining a timeline and level of effort based on the impact and prioritization of each identified finding.		x	x
18	18.4	Network	Protect	Validate Security Measures	Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.			x
18	18.5	Network	Detect	Perform Periodic Internal Penetration Tests	Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.			x

CIS Controls Status Report

Control	Sub-Control	Description	Status
1	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Effective
	1.2	Address Unauthorized Assets	Effective
2	2.1	Establish and Maintain a Software Inventory	Effective
	2.2	Ensure Authorized Software is Currently Supported	Partial
	2.3	Address Unauthorized Software	Partial
3	3.1	Establish and Maintain a Data Management Process	Partial
	3.2	Establish and Maintain a Data Inventory	Partial
	3.3	Configure Data Access Control Lists	Effective
	3.4	Enforce Data Retention	Partial
	3.5	Securely Dispose of Data	Implemented – Validation Pending
	3.6	Encrypt Data on End-User Devices	Partial
4	4.1	Establish and Maintain a Secure Configuration Process	Effective
	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Partial
	4.3	Configure Automatic Session Locking on Enterprise Assets	Effective
	4.4	Implement and Manage a Firewall on Servers	Effective
	4.5	Implement and Manage a Firewall on End-User Devices	Effective
	4.6	Securely Manage Enterprise Assets and Software	Effective
	4.7	Manage Default Accounts on Enterprise Assets and Software	Effective
5	5.1	Establish and Maintain an Inventory of Accounts	Effective
	5.2	Use Unique Passwords	Effective
	5.3	Disable Dormant Accounts	Effective
	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Effective
6	6.1	Establish an Access Granting Process	Partial
	6.2	Establish an Access Revoking Process	Effective
	6.3	Require MFA for Externally-Exposed Applications	Partial
	6.4	Require MFA for Remote Network Access	Implemented – Validation Pending
	6.5	Require MFA for Administrative Access	Partial
7	7.1	Establish and Maintain a Vulnerability Management Process	Implemented – Validation Pending
	7.2	Establish and Maintain a Remediation Process	Implemented – Validation Pending
	7.3	Perform Automated Operating System Patch Management	Effective
	7.4	Perform Automated Application Patch Management	Implemented – Validation Pending
8	8.1	Establish and Maintain an Audit Log Management Process	Implemented – Validation Pending
	8.2	Collect Audit Logs	Partial
	8.3	Ensure Adequate Audit Log Storage	Implemented – Validation Pending

CIS Controls Status Report

Control	Sub-Control	Description	Status
9	9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Partial
	9.2	Use DNS Filtering Services	Effective
10	10.1	Deploy and Maintain Anti-Malware Software	Effective
	10.2	Configure Automatic Anti-Malware Signature Updates	Effective
	10.3	Disable Autorun and Autoplay for Removable Media	Effective
11	11.1	Establish and Maintain a Data Recovery Process	Implemented – Validation Pending
	11.2	Perform Automated Backups	Effective
	11.3	Protect Recovery Data	Effective
	11.4	Establish and Maintain an Isolated Instance of Recovery Data	Effective
12	12.1	Ensure Network Infrastructure is Up-to-Date	Implemented – Validation Pending
14	14.1	Establish and Maintain a Security Awareness Program	Partial
	14.2	Train Workforce Members to Recognize Social Engineering Attacks	Partial
	14.3	Train Workforce Members on Authentication Best Practices	Implemented – Validation Pending
	14.4	Train Workforce on Data Handling Best Practices	Implemented – Validation Pending
	14.5	Train Workforce Members on Causes of Unintentional Data Exposure	Implemented – Validation Pending
	14.6	Train Workforce Members on Recognizing and Reporting Security Incidents,Train workforce members to be able to recognize a potential incident and be able to report such an incident.	Implemented – Validation Pending
	14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Implemented – Validation Pending
	14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Implemented – Validation Pending
15	15.1	Establish and Maintain an Inventory of Service Providers	Partial
17	17.1	Designate Personnel to Manage Incident Handling	Partial
	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Partial
	17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	Partial

IT/Cyber Security Activities Completed/In Process in FY26:

- Incident response planning
- Revise technical processes for staff and hardware onboarding
- Began formation of onboarding process
- Revise technical offboarding processes
- Began discussions of offboarding process
- Completion of Windows 11 Operating System deployment
- Planned upgrades completed on all but 2 workstation / hosts. Remaining to be completed by 6/30/26
- Upgrading of vendor applications after migration to datacenter
- Completed deployment of employee cyber security training
- Began deployment of cyber security training; continuing roll-out.
- Continued security culture development with focus on “AI” based threats
- Evaluation of cyber-AI threat detection including endpoint protection
- Consolidation and optimization of virtual servers during migration to datacenter platform
- Completed primary server deployment

Proposed IT/Cyber Security Activities for FY27:

- Incidence Response Planning
- Continue formation of staff, hardware onboarding
- Continue formation of offboard process
- Upgrade backup systems
- Implementation of upgraded endpoint protection
- Continue Cyber Security Awareness Training rollout
- Continued vulnerability scans and remediation
- Continued incident response development
- Evaluate data encryption policy
- Continue cyber security training roll-out
- Review options for cyber security review

AGENDA ITEM #4

AGENDA ITEM: 4

MEETING DATE: September 9, 2026

I. NATURE OF ITEM

Consideration of Transferring Additional Funds from Community West Bank ICS Money Market Fund to California Cooperative Liquid Asset Securities System ("CA-CLASS") Term Series II Portfolios

II. BACKGROUND INFORMATION

On August 3, 2026, the Board passed Resolution No. 26-739 authorizing investment of District Funds in the CA-CLASS Term Series II Portfolio. CA-CLASS has established Term Series II Portfolios as an alternative investment for Prime Fund participants. Each Term Series II Portfolio has a portfolio-specific final maturity date of not more than two (2) years. Each Term Series II Portfolio offers a fixed interest rate based on the redemption date selected by the participant. An investment of a minimum of sixty (60) days and a maximum of one (1) year is available. This investment is much like a Certificate of Deposit. The Community West Bank ICS Money Market Account is currently paying an interest rate of 3.6%, and the CA-CLASS Term Series II Portfolios are currently quoting an interest rate of over 4.2%. The difference in these rates, 0.6%, could generate an additional $6,000 in annual interest income per $1M invested.

III. COMMENTS AND RECOMMENDATIONS

Staff has moved $5M from the CA-CLASS Prime fund into the Term Series II account (12-month term at 4.24%). Based on a cursory review of planned capital fund expenditures for FY27, is appears that the District can move up to $10M of additional funds from the Community West ICS Money Market Account to the CA CLASS Term Series II account for a 12-month term. If the Board wishes to authorize the transfer of District funds to the CA-CLASS Term Series II portfolios from the District Funds held at Community West Bank, it is recommended that the Board direct staff to do so and specify the amount of such a transfer.

IV. REFERENCE MATERIAL

None

GENERAL MANAGER’S REPORT

GOLETA SANITARY DISTRICT
GENERAL MANAGER'S REPORT

The following summary report describes the District's activities from August 18, 2026, through September 9, 2026. It provides updated information on significant activities under three major categories: Collection System, Treatment/Reclamation and Disposal Facilities, and General and Administration Items.

1. COLLECTION SYSTEM REPORT

LINES CLEANING
Staff continues routine lines cleaning in the area of North La Cumbre and Foothill Roads. Staff has also been conducting priority lines cleaning throughout the District.

CCTV INSPECTION
Staff has been conducting routine CCTV inspections in the area of Encore Drive and Modoc Road. Staff has also been conducting priority CCTV inspections throughout the District.

REPAIR AND MAINTENANCE
Granite Construction has finished the adjustment of the District's 32 manholes and six cleanouts that were part of the County of Santa Barbara's Fiscal Year 25-26 South and Central County Pavement Rehabilitation Project. Staff provided 19 replacement frames and covers and inspected the work.

Staff replaced the pigtail connector on the CCTV Inspection Van equipment, which links the camera transporter to the camera inspection cable.

CUESTA VERDE ODOR ISSUE
Staff has resumed gas monitor readings on Cuesta Verde in response to an ongoing odor issue associated with the force main lateral from the Santa Barbara Wildlife Care Network's effluent pumpstation. The District's cleanout and manhole frames and covers on Cuesta Verde were previously paved over and have now been adjusted to grade by Granite Construction as part of the County of Santa Barbara's paving project.

GREASE AND OIL INSPECTIONS
Staff continues with annual Grease and Oil inspections at food service establishments within the District.

COLLECTION SYSTEM MAINTENANCE TECH I RECRUITMENT (CSMT I)
Staff conducted the second round of interviews for the open CSMT on August 18 and 19, 2026. Staff is preparing an offer letter for one of the candidates. There were four candidates under consideration.

2. TREATMENT, RECLAMATION AND DISPOSAL FACILITIES REPORT
The Plant flow for the month August has averaged 4.48 MGD (million gallons per day). Work on the BESP Phase 1 continues, and control programming and testing is ongoing. Gateway has begun removing the spoils pile from the Plant. Planning for Digester #4 startup continues.

The Reclamation Facility has produced an average of 1.74 MGD for the month of August.

3. GENERAL AND ADMINISTRATIVE ITEMS

Financial Report

The District account balances as of September 9, 2026, shown below, are approximations to the nearest dollar and indicate the overall funds available to the District at this time.

Operating Checking Accounts:	$	309,666
Investment Accounts (including interest earned):	$	44,108,636
Total District Funds:	$	44,418,302

The following transactions are reported herein for the period 08/18/2026 – 09/09/2026

Regular, Overtime, Cash-outs, and Net Payroll:	$	179,726
Claims:	$	600,257
Total Expenditures:	$	779,983
Total Deposits:	$	301,597

Transfers of funds:

LAIF to Community West Bank Operational (CWB):	$	- 0 -
CWB Operational to CWB Money Market:	$	- 0 –
CWB Money Market to CWB Operational:	$	1,500,000
CWB Operational to CA-Class Investment Account	$	1,000,000
CA-Class Investment Account to CWB Operational	$	- 0 -

The District's investments comply with the District's Investment Policy adopted per Resolution No. 16-606. The District has adequate funds to meet the next six months of normal operating expenses.

Local Agency Investment Fund (LAIF)

LAIF Monthly Statement – August, 2026
LAIF Quarterly Report – Previously reported
PMIA/LAIF Performance – Previously reported
PMIA Effective Yield – Previously reported

Community West Bank (CWB)

CWB Money Market and ICS Accounts – August, 2026

CA-Class Investment Account

CA-Class Investment Account – August, 2026

Deferred Compensation Accounts

CalPERS 457 Deferred Compensation Plan – Previously reported
Lincoln 457 Deferred Compensation Plan – August, 2026

Personnel

A verbal personnel update will be provided at the meeting.

Future Agenda Items
Review of Draft 2027 Strategic Plan

Upcoming Calendar of Events:
Lemon Festival Outreach Event- September 26-27, 2026

State of California
Office of the
State Treasurer

LAIF Monthly Statements

LAIF Monthly Statement

GOLETA SANITARY DISTRICT
GENERAL MANAGER
ONE WILLIAM MOFFETT PLACE
GOLETA, CA 93117

LAIF Account #: 70-42-002
August 2026 Statement

No transactions were found for this reporting period.

Account Summary

Beginning Balance:	4,367.37
Total Deposit:	0.00
Total Withdrawal:	0.00
Ending Balance:	4,367.37

Community West Bank

Statement Ending 08/31/2026

7100 N. Financial Dr. STE 101
Fresno, CA 93720

GOLETA SANITARY DISTRICT
1 WILLIAM MOFFETT PL
GOLETA CA 93117-3901

Summary of Accounts

Account Type	Account Number	Ending Balance
PUBLIC MONEY MARKET	XXXXXXXXXXXX554	$250,000.00

PUBLIC MONEY MARKET - XXXXXXXXXXXX554

Account Summary

Date	Description	Amount
08/01/2026	**Beginning Balance**	**$250,000.00**
	3 Credit(s) This Period	$1,000,764.38
	3 Debit(s) This Period	$1,000,764.38
08/31/2026	**Ending Balance**	**$250,000.00**

Interest Summary

Description	Amount
Interest Earned From 08/01/2026 Through 08/31/2026	
Annual Percentage Yield Earned	3.66%
Interest Days	31
Interest Earned	$764.38
Interest Paid This Period	$764.38
Interest Paid Year-to-Date	$5,991.78
Minimum Balance	$250,000.00
Average Ledger Balance	$250,000.00

Other Credits

Date	Description	Amount
08/04/2026	ICS WITHDRAWAL	$750,000.00
08/28/2026	TRANSFER FROM ICS SHADOW DDA ACCOUNT XXXXXXXXXXX8650	$250,000.00
08/31/2026	INTEREST	$764.38
		3 item(s) totaling $1,000,764.38

Electronic Debits

Date	Description	Amount
08/04/2026	Internet Transfer to xxx5538	$750,000.00
08/28/2026	Internet Transfer to xxx5538	$250,000.00
		2 item(s) totaling $1,000,000.00

PUBLIC MONEY MARKET - XXXXXXXXXXXX554 (continued)

Other Debits

Date	Description	Amount
08/31/2026	TRANSFER TO ICS SHADOW DDA ACCOUNT XXXXXXXXXXXX8650	$764.38
		1 item(s) totaling $764.38

Overdraft and Returned Item Fees

	Total for this period	Total year-to-date
Total Overdraft Fees	$0.00	$0.00
Total Returned Item Fees	$0.00	$0.00

61765

Community West Bank
7100 N Financial Dr Ste 101
Fresno, CA 93720

RETURN SERVICE REQUESTED

145718-31A
Goleta Sanitary District
One William Moffett Place
Goleta, CA 93117

Community West Bank

Contact Us
559-298-1775
www.communitywestbank.com

Account
Goleta Sanitary District

Date
08/31/2026

IntraFi Cash Service℠, or ICS®, Monthly Statement

The following information is a summary of activity in your account(s) for the month of August 2026 and the list of FDIC-insured institution(s) that hold your deposits as of the date indicated. These deposits have been placed by us, as your agent and custodian, in deposit accounts through IntraFi Cash Service. Funds in your deposit accounts at the FDIC-insured institutions at which your funds have been placed will be "deposits," as defined by federal law. Certain conditions must be satisfied for "pass-through" FDIC deposit insurance coverage to apply. To meet the conditions for pass-through FDIC deposit insurance, deposit accounts at FDIC-insured banks in IntraFi's network that hold deposits placed using an IntraFi service are titled, and deposit account records are maintained, in accordance with FDIC regulations for pass-through coverage.

Summary of Accounts

Account ID	Deposit Option	Interest Rate	Opening Balance	Ending Balance
*********554	Demand	3.60%	$38,969,671.41	$38,087,739.59
TOTAL			**$38,969,671.41**	**$38,087,739.59**

DETAILED ACCOUNT OVERVIEW

Account ID: *********554
Account Title: Goleta Sanitary District

Account Summary - Demand

Statement Period	8/1-8/31/2026
Previous Period Ending Balance	$38,969,671.41
Total Program Deposits	764.38
Total Program Withdrawals	(1,000,000.00)
Interest Capitalized	117,303.80
Current Period Ending Balance	**$38,087,739.59**

Average Daily Balance	$38,312,988.75
Interest Rate at End of Statement Period	3.60%
Annual Percentage Yield Earned	3.67%
YTD Interest Paid	964,454.47

Account Transaction Detail

Date	Activity Type	Amount	Balance
08/03/2026	Deposit	$764.38	$38,970,435.79
08/05/2026	Withdrawal	(750,000.00)	38,220,435.79
08/25/2026	Interest Capitalization	561.13	38,220,996.92
08/31/2026	Withdrawal	(250,000.00)	37,970,996.92
08/31/2026	Interest Capitalization	116,742.67	38,087,739.59

Summary of Balances as of August 31, 2026

FDIC-Insured Institution	City/State	FDIC Cert No.	Balance
Alerus Financial, N.A.	Grand Forks, ND	3931	$247,756.47
Amalgamated Bank	New York, NY	622	247,756.47
Amerant Bank, N.A.	Coral Gables, FL	22953	247,756.47
Ameris Bank	Atlanta, GA	20504	49.01
Apple Bank	New York, NY	16068	247,756.47
Associated Bank, N.A.	Green Bay, WI	5296	247,756.47
Atlantic Union Bank	Glen Allen, VA	34589	247,756.47
Avidbank	San Jose, CA	57510	247,756.47
BOKF, National Association	Tulsa, OK	4214	247,756.47
Banc of California	Los Angeles, CA	24045	247,756.47
Banesco USA	Miami, FL	57815	0.11
Bank 7	Oklahoma City, OK	4147	247,756.47
Bank OZK	Little Rock, AR	110	247,756.47
Bank of Baroda	New York, NY	33681	247,756.47
Bank of Central Florida	Lakeland, FL	58479	247,756.47
Bank of China	New York, NY	33653	247,756.47
Bank of India	New York, NY	33648	247,707.45
Bank of New Hampshire	Laconia, NH	18012	49.01
Bank of the Sierra	Porterville, CA	22597	247,707.46
BankUnited	Miami Lakes, FL	58979	247,721.18
Bankers Trust Company	Des Moines, IA	953	247,756.47
Banterra Bank	Marion, IL	17514	247,756.47

DETAILED ACCOUNT OVERVIEW

Account ID: *********554
Account Title: Goleta Sanitary District

Summary of Balances as of August 31, 2026

FDIC-Insured Institution	City/State	FDIC Cert No.	Balance
Bar Harbor Bank & Trust	Bar Harbor, ME	11971	247,756.47
Barclays Bank Delaware	Wilmington, DE	57203	247,756.47
Bell Bank	Fargo, ND	19581	247,756.47
Benchmark Community Bank	Kenbridge, VA	20484	247,756.47
Beneficial State Bank	Oakland, CA	58490	247,756.47
Bridgewater Bank	Saint Louis Park, MN	58210	247,756.47
Busey Bank	Champaign, IL	16450	247,756.47
CIBC Bank USA	Chicago, IL	33306	247,756.47
California Bank of Commerce, N.A.	San Diego, CA	57044	247,756.47
Cathay Bank	Los Angeles, CA	18503	247,756.46
Cedar Rapids Bank and Trust Company	Cedar Rapids, IA	57244	247,756.47
Centennial Bank	Conway, AR	11241	247,756.47
Choice Financial Group	Grafton, ND	9423	247,756.47
Citizens Bank, National Association	Providence, RI	57957	247,756.40
City National Bank	Beverly Hills, CA	17281	247,756.47
City National Bank of Florida	Miami, FL	20234	247,756.47
Coastal Community Bank	Everett, WA	34403	43.36
Columbia Bank	Roseburg, OR	17266	247,756.47
Commerce Bank	Kansas City, MO	24998	247,756.47
Commercial Bank of California	Irvine, CA	57417	247,756.47
ConnectOne Bank	Englewood Cliffs, NJ	57919	247,756.47
Cross River Bank	Teaneck, NJ	58410	0.05
Customers Bank	Malvern, PA	34444	97.87
Dacotah Bank	Aberdeen, SD	17437	247,756.47
Dime Commercial Bank	Hauppauge, NY	6976	247,756.47
EagleBank	Silver Spring, MD	34742	180,746.79
East West Bank	Pasadena, CA	31628	49.01
Eastern Bank	Boston, MA	32773	247,756.47
Encore Bank	Little Rock, AR	34562	247,756.47
Enterprise Bank & Trust	Clayton, MO	27237	247,756.47
Equity Bank	Andover, KS	25858	247,756.47
Erebor Bank, N.A.	Columbus, OH	59378	0.12
Farmers Bank & Trust Company	Magnolia, AR	1291	247,756.47
Farmers National Bank of Canfield	Canfield, OH	6540	247,194.96
Fifth Third Bank	Cincinnati, OH	6672	247,756.47
First Bank	Creve Coeur, MO	12229	247,756.47
First Bank Chicago	Highland Park, IL	17470	247,756.47
First Carolina Bank	Rocky Mount, NC	35530	247,756.47
First Commonwealth Bank	Indiana, PA	7468	247,756.47

DETAILED ACCOUNT OVERVIEW

Account ID: *********554
Account Title: Goleta Sanitary District

Summary of Balances as of August 31, 2026

FDIC-Insured Institution	City/State	FDIC Cert No.	Balance
First Financial Bank	Abilene, TX	3066	247,756.47
First Horizon Bank	Memphis, TN	4977	247,756.47
First International Bank & Trust	Watford City, ND	10248	247,756.47
First Interstate Bank	Billings, MT	1105	247,756.47
First Merchants Bank	Muncie, IN	4365	247,756.47
First Mid Bank & Trust N.A.	Mattoon, IL	3705	247,756.47
First National Bank of Michigan	Kalamazoo, MI	58259	247,756.47
First National Bank of Omaha	Omaha, NE	5452	247,756.47
First National Bank of Pennsylvania	Greenville, PA	7888	247,756.47
First State Community Bank	Farmington, MO	17323	247,756.47
First United Bank and Trust Company	Durant, OK	4239	247,756.46
First-Citizens Bank & Trust Company	Raleigh, NC	11063	247,756.47
FirstBank	Nashville, TN	8663	247,756.47
Five Star Bank	Warsaw, NY	659	247,756.47
Flagstar Bank, N.A.	Hicksville, NY	32541	247,756.47
Fulton Bank, N.A.	Lancaster, PA	7551	247,756.47
Glacier Bank	Kalispell, MT	30788	247,756.47
Great Southern Bank	Reeds Spring, MO	29546	247,756.47
Guaranty Bank	Springfield, MO	58892	247,756.47
Gulf Coast Bank and Trust Company	New Orleans, LA	32974	247,756.47
Hanover Community Bank	Mineola, NY	58675	247,756.47
Heritage Bank	Olympia, WA	29012	247,756.47
Home Bank, N.A.	Lafayette, LA	28094	97.87
INB	Springfield, IL	3664	247,756.47
INTRUST Bank NA	Wichita, KS	4799	247,756.47
Independent Bank	Ionia, MI	27811	247,756.47
InterBank	Oklahoma City, OK	27210	247,756.47
Inwood National Bank	Dallas, TX	19080	247,756.47
Israel Discount Bank of New York	New York City, NY	19977	247,756.47
KeyBank National Association	Cleveland, OH	17534	247,756.47
Liberty National Bank	Lawton, OK	11522	247,756.47
Live Oak Banking Company	Wilmington, NC	58665	247,756.45
MVB Bank, Inc	Fairmont, WV	34603	247,756.47
Machias Savings Bank	Machias, ME	19531	49.01
Manufacturers and Traders Trust Company	Buffalo, NY	588	247,756.47
Mechanics Bank	Walnut Creek, CA	1768	247,756.47
Mercantile Bank	Grand Rapids, MI	34598	247,756.47
Merchants Bank of Indiana	Carmel, IN	8056	247,756.47
MidFirst Bank	Oklahoma City, OK	4063	0.12

DETAILED ACCOUNT OVERVIEW

Account ID: *********554
Account Title: Goleta Sanitary District

Summary of Balances as of August 31, 2026

FDIC-Insured Institution	City/State	FDIC Cert No.	Balance
Midland States Bank	Effingham, IL	1040	0.12
Minnwest Bank	Redwood Falls, MN	16958	247,568.22
Morton Community Bank	Morton, IL	18429	247,756.47
NBH Bank	Greenwood Village, CO	59052	247,756.47
NBT Bank, National Association	Norwich, NY	7230	247,756.47
Northeast Bank	Lewiston, ME	19690	247,756.47
Northpointe Bank	Grand Rapids, MI	34953	247,756.47
Northwest Bank	Warren, PA	28178	247,756.47
OceanFirst Bank	Red Bank, NJ	28359	247,743.71
Old National Bank	Evansville, IN	3832	247,756.46
Origin Bank	Ruston, LA	12614	247,756.47
Outdoor Bank	Manhattan, KS	17685	247,756.47
Park National Bank	Newark, OH	6653	247,756.47
Peoples National Bank, N.A.	Mt. Vernon, IL	3809	247,756.47
Pinnacle Bank	Omaha, NE	10634	247,756.47
Pinnacle Bank	Nashville, TN	35583	247,756.47
PlainsCapital Bank	Lubbock, TX	17491	247,756.47
Planters Bank, Inc.	Hopkinsville, KY	34254	247,756.47
Popular Bank	New York, NY	34967	247,756.47
Preferred Bank	Los Angeles, CA	33539	247,756.47
Primis Bank	Mclean, VA	57968	247,756.47
Prosperity Bank	El Campo, TX	16835	247,756.47
Provident Bank	Jersey City, NJ	12010	247,756.47
Quad City Bank and Trust Company	Bettendorf, IA	33867	247,756.47
RCB Bank	Claremore, OK	15399	247,756.47
Raymond James Bank	St. Petersburg, FL	33893	247,756.47
Renasant Bank	Tupelo, MS	12437	0.03
River City Bank	Sacramento, CA	18983	247,756.47
Rockland Trust Company	Rockland, MA	9712	247,756.47
Santander Bank, N.A.	Wilmington, DE	29950	247,756.47
Seacoast National Bank	Stuart, FL	131	247,756.47
Security First Bank	Rapid City, SD	5415	247,756.47
Shore United Bank, N.A.	Easton, MD	4832	247,756.47
Simmons Bank	Pine Bluff, AR	3890	247,756.47
South State Bank, N.A.	Winter Haven, FL	33555	247,756.47
SouthEast Bank	Farragut, TN	57348	247,756.47
Southern Bank	Poplar Bluff, MO	28332	247,756.47
State Bank of India	New York City, NY	33682	247,756.47
Stifel Bank	St. Louis, MO	57358	247,756.47

DETAILED ACCOUNT OVERVIEW

Account ID: *********554
Account Title: Goleta Sanitary District

Summary of Balances as of August 31, 2026

FDIC-Insured Institution	City/State	FDIC Cert No.	Balance
Stock Yards Bank & Trust Company	Louisville, KY	258	713.16
Sunflower Bank NA	Salina, KS	4767	247,756.47
Texas Capital Bank	Dallas, TX	34383	247,756.47
The Camden National Bank	Camden, ME	4255	247,756.47
The Farmers & Merchants State Bank	Archbold, OH	5969	247,756.47
The Huntington National Bank	Columbus, OH	6560	247,756.47
Tompkins Bank & Trust	Ithaca, NY	609	49.01
Town Bank, N.A.	Hartland, WI	34717	247,707.46
TowneBank	Portsmouth, VA	35095	247,756.47
Tradition Capital Bank	Edina, MN	58057	247,756.47
Traditional Bank, Inc.	Mount Sterling, KY	2711	247,756.47
Tri Counties Bank	Chico, CA	21943	247,756.47
TriState Capital Bank	Pittsburgh, PA	58457	247,756.47
Truist Bank	Charlotte, NC	9846	247,756.47
Trustmark Bank	Jackson, MS	4988	247,756.47
UMB Bank, National Association	Kansas City, MO	8273	247,756.47
UniBank for Savings	Whitinsville, MA	90290	247,756.47
Union Bank & Trust	Lincoln, NE	13421	247,756.47
United Bank	Fairfax, VA	22858	247,756.47
United Community Bank	Greenville, SC	16889	247,756.47
Univest Bank and Trust Co.	Souderton, PA	7759	247,756.47
Valley National Bank	Morristown, NJ	9396	247,756.47
WaFd Bank	Seattle, WA	28088	247,756.47
Waterford Bank, N.A.	Toledo, OH	58433	247,756.47
WesBanco Bank, Inc.	Wheeling, WV	803	247,756.47
Western Alliance Bank	Phoenix, AZ	57512	247,756.47
Wilmington Savings Fund Society, FSB	Wilmington, DE	17838	247,756.47
Woodforest Natl Bank	The Woodlands, TX	23220	247,756.47
Zions Bancorporation, N. A.	Salt Lake City, UT	2270	247,756.47
b1BANK	Baton Rouge, LA	58228	247,756.47

California CLASS

Summary Statement

August 31, 2026

0000029-0000151 PDFT 221701

Goleta Sanitary District
1 William Moffett Place
Goleta, CA 93117

California CLASS

California CLASS

Average Monthly Yield: 3.7484%

	Beginning Balance	Contributions	Withdrawals	Income Earned	Income Earned YTD	Average Daily Balance	Month End Balance
Goleta Sanitary District	5,996,678.04	0.00	0.00	19,087.01	147,046.65	5,997,293.75	6,015,765.05
TOTAL	**5,996,678.04**	**0.00**	**0.00**	**19,087.01**	**147,046.65**	**5,997,293.75**	**6,015,765.05**

Goleta Sanitary District

Account Summary

Average Monthly Yield: 3.7484%

	Beginning Balance	Contributions	Withdrawals	Income Earned	Income Earned YTD	Average Daily Balance	Month End Balance
California CLASS	5,996,678.04	0.00	0.00	19,087.01	147,046.65	5,997,293.75	6,015,765.05

Transaction Activity

Transaction Date	Transaction Description	Contributions	Withdrawals	Balance	Transaction Number
08/01/2026	Beginning Balance			5,996,678.04	
08/31/2026	Income Dividend Reinvestment	19,087.01			
08/31/2026	Ending Balance			6,015,765.05	

California CLASS

	California CLASS	
Date	Dividend Rate	Daily Yield
08/01/2026	0.000000000	3.7567%
08/02/2026	0.000205844	3.7567%
08/03/2026	0.000102625	3.7458%
08/04/2026	0.000102533	3.7425%
08/05/2026	0.000102638	3.7463%
08/06/2026	0.000102606	3.7451%
08/07/2026	0.000307731	3.7441%
08/08/2026	0.000000000	3.7441%
08/09/2026	0.000000000	3.7441%
08/10/2026	0.000102355	3.7360%
08/11/2026	0.000102538	3.7426%
08/12/2026	0.000102505	3.7414%
08/13/2026	0.000102463	3.7399%
08/14/2026	0.000307629	3.7428%
08/15/2026	0.000000000	3.7428%
08/16/2026	0.000000000	3.7428%
08/17/2026	0.000102638	3.7463%
08/18/2026	0.000102926	3.7568%
08/19/2026	0.000102823	3.7530%
08/20/2026	0.000102446	3.7393%
08/21/2026	0.000307422	3.7403%
08/22/2026	0.000000000	3.7403%
08/23/2026	0.000000000	3.7403%
08/24/2026	0.000102825	3.7531%
08/25/2026	0.000102852	3.7541%
08/26/2026	0.000103055	3.7615%
08/27/2026	0.000102991	3.7592%
08/28/2026	0.000308967	3.7591%
08/29/2026	0.000000000	3.7591%
08/30/2026	0.000000000	3.7591%
08/31/2026	0.000103168	3.7656%

Performance results are shown net of all fees and expenses and reflect the reinvestment of dividends and other earnings. Many factors affect performance including changes in market conditions and interest rates and in response to other economic, political, or financial developments. Investment involves risk including the possible loss of principal. No assurance can be given that the performance objectives of a given strategy will be achieved. **Past performance is no guarantee of future results. Any financial and/or investment decision may incur losses.**

Lincoln Financial Group®
Multi-Fund® Select

Performance Update

MultiFund

Quoted performance data represents past performance. Past performance does not guarantee nor predict future performance. Current performance may be lower or higher than the performance data quoted. Please keep in mind that double-digit returns are highly unusual and cannot be sustained.

Variable products are sold by prospectus. Consider the investment objectives, risks, charges, and expenses of the variable product and its underlying investment options carefully before investing. The prospectus contains this and other information about the variable product and its underlying investment options. Please review the prospectus available online for additional information. Read it carefully before investing.

Investment return and principal value of an investment will fluctuate so that an investor's unit values, when redeemed, may be worth more or less than their original cost.

Monthly hypothetical performance adjusted for contract fees *

								Average Annual Total Return (%) as of 8/31/2026				
Investment Options		Inception Date	Change from Previous Day 09/02/2026	YTD as of 09/02/2026	YTD as of 08/31/2026	1 Mo as of 08/31/2026	3 Mo as of 08/31/2026	1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
Maximum Capital Appreciation												
DWS Alternative Asset Allocation VIP Portfolio - Class B[1, 2, 3, 4, 5]	MCA	02/02/2009	0.00	9.14	9.38	1.40	-0.94	12.37	8.53	3.64	3.86	4.30
LVIP Baron Growth Opportunities Fund - Service Class[8, 9]	MCA	10/01/1998	-0.28	-5.68	-3.89	5.58	8.19	-9.45	-2.70	-4.70	6.54	8.81
LVIP Franklin Templeton Multi-Factor Emerging Markets Equity Fund - Service Class[1, 7, 9]	MCA	06/18/2008	-0.33	23.55	24.58	3.65	-1.88	38.58	22.99	10.28	7.58	4.67
LVIP Nomura SMID Cap Core Fund - Service Class[8, 9]	MCA	07/12/1991	0.68	16.01	16.21	-0.19	1.81	21.58	14.57	7.33	9.23	8.98
LVIP State Street Small-Cap Index Fund - Service Class[8, 9, 22]	MCA	04/18/1986	1.13	18.69	18.80	0.82	1.19	24.51	15.63	5.14	8.75	6.84

Printed on 09/03/2026 03:02PM ET

Performance Update

MultiFund

Monthly hypothetical performance adjusted for contract fees *

Investment Options		Inception Date	Change from Previous Day 09/02/2026	YTD as of 09/02/2026	YTD as of 08/31/2026	1 Mo as of 08/31/2026	3 Mo as of 08/31/2026	Average Annual Total Return (%) as of 8/31/2026 1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
LVIP T. Rowe Price Structured Mid-Cap Growth Fund - Service Class[8, 9]	MCA	02/03/1994	-0.35	1.15	3.37	1.69	-0.87	0.08	13.61	3.97	11.25	7.02
Long Term Growth												
American Funds® IS EUPAC Fund - Class 2[1]	LTG	05/01/1990	-0.77	15.07	16.74	3.30	1.87	27.74	15.96	4.75	7.04	6.71
American Funds® IS Global Growth Fund - Class 2[1]	LTG	04/30/1997	-0.13	15.33	16.26	1.20	-2.42	23.81	18.83	7.05	12.49	9.53
American Funds® IS Growth Fund - Class 2	LTG	02/08/1984	0.59	5.78	6.22	4.48	-1.33	11.71	21.49	10.11	16.91	12.34
Fidelity® VIP Contrafund® Portfolio - Service Class 2	LTG	01/03/1995	0.60	8.39	8.42	1.67	-0.53	14.13	22.38	11.32	14.75	11.10
Fidelity® VIP Growth Portfolio - Service Class 2	LTG	10/09/1986	0.61	9.90	10.41	3.59	-2.81	15.30	19.92	10.46	16.99	10.40
LVIP BlackRock Real Estate Fund - Service Class[1, 8, 9, 13, 14]	LTG	04/30/2007	-0.38	8.05	8.80	-3.34	-0.26	8.33	8.58	-1.02	2.45	1.15
LVIP Dimensional U.S. Core Equity 1 Fund - Service Class[9]	LTG	12/28/1981	0.63	13.84	13.93	1.92	2.34	19.34	18.01	10.39	12.83	9.87
LVIP Mondrian International Value Fund - Service Class[1, 9]	LTG	05/01/1991	-0.17	11.56	12.54	0.18	4.22	21.00	18.53	10.11	7.42	5.88
LVIP Nomura Mid Cap Value Fund - Service Class[8, 9]	LTG	12/28/1981	0.47	17.65	18.13	-1.48	1.12	22.68	16.94	9.55	10.00	10.13
LVIP State Street International Index Fund - Service Class[1, 9, 22, 23]	LTG	04/30/2008	0.15	11.92	12.89	1.84	3.57	20.07	16.51	7.76	7.92	3.49
LVIP State Street S&P 500 Index Fund - Service Class[9, 22, 24]	LTG	05/01/2000	0.46	11.74	12.03	2.59	1.30	18.61	19.26	11.13	13.67	6.87
LVIP Vanguard Domestic Equity ETF Fund - Service Class[3, 4]	LTG	04/29/2011	0.46	12.35	12.70	2.57	1.65	18.59	18.41	10.06	12.93	11.46

Printed on 09/03/2026 03:02PM ET

Multi-Fund® Select

Performance Update

MultiFund

Monthly hypothetical performance adjusted for contract fees *

Investment Options		Inception Date	Change from Previous Day 09/02/2026	YTD as of 09/02/2026	YTD as of 08/31/2026	1 Mo as of 08/31/2026	3 Mo as of 08/31/2026	Average Annual Total Return (%) as of 8/31/2026 1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
LVIP Vanguard International Equity ETF Fund - Service Class[1, 3, 4]	LTG	04/29/2011	0.52	15.13	15.39	2.94	1.58	24.17	17.60	7.12	7.92	5.05
MFS® VIT Utilities Series - Service Class[8, 13]	LTG	01/03/1995	-0.25	1.25	0.48	-5.10	-5.16	4.81	9.19	4.65	6.98	9.07
Nomura VIP Small Cap Value Series - Service Class[8]	LTG	12/27/1993	1.01	16.29	16.38	-2.68	1.91	18.52	12.93	6.56	7.96	8.92
Growth and Income												
American Funds® IS Growth-Income Fund - Class 2	GI	02/08/1984	0.32	11.39	11.79	0.92	1.50	17.08	20.17	11.45	13.31	10.53
Fidelity® VIP Freedom 2020 Portfolio℠ - Service Class 2[3, 6]	GI	04/26/2005	0.15	5.04	5.29	0.93	-0.17	8.30	9.45	3.04	6.07	5.41
Fidelity® VIP Freedom 2025 Portfolio℠ - Service Class 2[3, 6]	GI	04/26/2005	0.29	6.07	6.33	1.08	-0.02	9.67	10.59	3.68	6.82	6.01
Fidelity® VIP Freedom 2030 Portfolio℠ - Service Class 2[3, 6]	GI	04/26/2005	0.28	6.87	7.18	1.21	0.14	10.85	11.59	4.31	7.77	6.40
Fidelity® VIP Freedom 2035 Portfolio℠ - Service Class 2[3, 6]	GI	04/08/2009	0.32	7.94	8.27	1.33	0.33	12.35	13.05	5.29	9.01	10.25
Fidelity® VIP Freedom 2040 Portfolio℠ - Service Class 2[3, 6]	GI	04/08/2009	0.36	9.92	10.29	1.57	0.67	15.06	15.24	6.74	10.07	10.95
Fidelity® VIP Freedom 2045 Portfolio℠ - Service Class 2[3, 6]	GI	04/08/2009	0.44	11.27	11.63	1.71	0.89	16.74	16.36	7.43	10.43	11.21
Fidelity® VIP Freedom 2050 Portfolio℠ - Service Class 2[3, 6]	GI	04/08/2009	0.45	11.53	11.89	1.75	0.98	17.02	16.45	7.48	10.45	11.30
LVIP BlackRock Equity Dividend Fund - Service Class[9]	GI	07/28/1988	0.32	16.44	16.21	0.58	7.17	22.83	12.80	7.31	7.75	7.69
LVIP JPMorgan Retirement Income Fund - Service Class[2, 9, 17]	GI	04/27/1983	0.23	4.48	4.70	0.94	0.13	7.78	8.85	3.16	4.20	6.12

Multi-Fund® Select

Performance Update

MultiFund

Monthly hypothetical performance adjusted for contract fees *

Investment Options		Inception Date	Change from Previous Day 09/02/2026	YTD as of 09/02/2026	YTD as of 08/31/2026	1 Mo as of 08/31/2026	3 Mo as of 08/31/2026	Average Annual Total Return (%) as of 8/31/2026: 1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
LVIP Nomura U.S. REIT Fund - Service Class[8, 9, 13, 14]	GI	05/04/1998	-0.39	14.17	14.64	-3.56	1.44	12.65	9.62	1.86	3.13	6.66
Income												
LVIP BlackRock Inflation Protected Bond Fund - Service Class[1, 9, 12]	I	04/30/2010	-0.01	0.86	0.95	-0.04	-0.79	0.74	2.94	1.01	1.55	1.40
LVIP Fidelity Institutional AM® Total Bond Fund - Service Class[9, 12]	I	05/16/2003	0.04	-1.03	-0.81	0.34	-0.95	0.79	3.04	-1.58	0.61	2.88
LVIP Franklin Templeton Core Bond Fund - Service Class[9, 12]	I	12/28/1981	0.06	-1.21	-1.00	0.26	-1.05	0.59	2.93	-1.68	0.30	5.45
LVIP Mondrian Global Income Fund - Service Class[1, 9, 10, 12]	I	05/04/2009	0.00	-1.16	-0.85	0.35	-0.87	-1.19	0.87	-4.02	-1.19	0.36
LVIP Nomura Diversified Floating Rate Fund - Service Class[9, 12, 18, 19]	I	04/30/2010	0.02	1.82	1.83	0.28	0.58	3.02	3.90	2.52	1.60	0.95
LVIP Nomura High Yield Fund - Service Class[9, 12, 20]	I	07/28/1988	0.04	0.93	1.07	0.90	0.52	3.01	6.46	2.29	3.65	4.97
LVIP State Street Bond Index Fund - Service Class[9, 12, 22]	I	04/30/2008	0.07	-1.48	-1.26	0.22	-1.11	0.21	2.43	-1.87	-0.19	1.14
PIMCO VIT Total Return Portfolio - Administrative Class[7, 12]	I	12/31/1997	0.12	-0.95	-0.75	0.32	-0.94	1.78	4.09	-0.93	0.83	3.33
Preservation of Capital												
LVIP Government Money Market Fund - Service Class 7-Day Current (Net/Gross) Yield as of 7/31/2026: 3.09%/3.72%[9, 16]	PC	01/07/1982	0.01	1.40	1.39	0.18	0.52	2.23	2.99	2.18	0.89	2.49
Risk Managed - Asset Allocation												

Lincoln Financial Group®
Multi-Fund® Select

Performance Update

MultiFund

Monthly hypothetical performance adjusted for contract fees *

Investment Options		Inception Date	Change from Previous Day 09/02/2026	YTD as of 09/02/2026	YTD as of 08/31/2026	1 Mo as of 08/31/2026	3 Mo as of 08/31/2026	Average Annual Total Return (%) as of 8/31/2026 1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
LVIP Global Conservative Allocation Managed Risk Fund - Service Class[1, 2, 3, 9, 15]	RMAA	05/03/2005	0.18	3.83	4.17	0.81	0.36	6.97	7.59	1.70	3.61	4.10
LVIP Global Growth Allocation Managed Risk Fund - Service Class[1, 2, 3, 9, 15]	RMAA	05/03/2005	0.24	7.93	8.42	1.35	1.17	12.69	11.85	3.85	5.45	4.47
LVIP Global Moderate Allocation Managed Risk Fund - Service Class[1, 2, 3, 9, 15]	RMAA	05/03/2005	0.21	6.38	6.83	1.20	0.81	10.59	10.12	3.00	4.75	4.38
LVIP State Street Global Tactical Allocation Managed Volatility Fund - Service Class[1, 2, 3, 9, 11]	RMAA	05/03/2005	0.30	7.96	8.24	1.71	1.02	13.12	11.61	4.84	5.78	4.09
Asset Allocation												
Fidelity® VIP Freedom 2055 Portfolio℠ - Service Class 2[3, 7]	AsA	04/11/2019	0.43	11.77	12.12	1.78	1.04	17.28	16.54	7.53	N/A	10.96
Fidelity® VIP Freedom 2060 Portfolio℠ - Service Class 2[3, 7]	AsA	04/11/2019	0.44	11.80	12.23	1.82	1.07	17.42	16.57	7.54	N/A	10.99
LVIP BlackRock Global Allocation Fund - Service Class[1, 2, 9]	AsA	04/26/2019	0.24	6.35	6.84	1.46	0.06	12.33	12.62	4.77	N/A	7.53
LVIP T. Rowe Price 2020 Fund - Service Class[3, 6, 9]	AsA	05/01/2007	0.25	6.06	6.32	1.27	0.45	10.01	10.08	3.71	5.85	4.12
LVIP T. Rowe Price 2030 Fund - Service Class[3, 6, 9]	AsA	05/01/2007	0.30	7.63	7.93	1.56	0.74	12.47	11.98	4.83	7.07	4.64
LVIP T. Rowe Price 2040 Fund - Service Class[3, 6, 9]	AsA	05/01/2007	0.39	10.81	11.15	2.04	1.34	17.03	15.16	6.94	8.75	5.17
LVIP T. Rowe Price 2050 Fund - Service Class[3, 6, 9]	AsA	04/29/2011	0.44	12.38	12.74	2.26	1.67	19.25	16.64	7.91	9.73	6.77

Lincoln Financial Group®

Multi-Fund® Select

Performance Update

MultiFund

Monthly hypothetical performance adjusted for contract fees *

Investment Options		Inception Date	Change from Previous Day 09/02/2026	YTD as of 09/02/2026	YTD as of 08/31/2026	1 Mo as of 08/31/2026	3 Mo as of 08/31/2026	Average Annual Total Return (%) as of 8/31/2026 1 Yr	3 Yr	5 Yr	10 Yr	Since Incep.
LVIP T. Rowe Price 2060 Fund - Service Class[3, 6, 9]	AsA	04/30/2020	0.45	12.58	12.94	2.28	1.70	19.46	16.75	8.00	N/A	13.76
Risk Managed - US Large Cap												
LVIP BlackRock Dividend Value Managed Volatility Fund - Service Class[9, 10, 11]	RMUSL	02/03/1994	0.38	19.25	18.99	1.42	7.12	23.91	15.33	9.16	9.03	7.02
LVIP Blended Large Cap Growth Managed Volatility Fund - Service Class[9, 10, 11]	RMUSL	02/03/1994	0.63	0.78	1.34	2.71	-3.39	5.92	13.48	6.32	11.08	7.20
Risk Managed - US Mid Cap												
LVIP Blended Mid Cap Managed Volatility Fund - Service Class[8, 9, 10, 11]	RMUSM	05/01/2001	-0.17	1.51	3.52	1.35	-0.62	-0.27	9.04	1.60	8.78	4.42
LVIP JPMorgan Select Mid Cap Value Managed Volatility Fund - Service Class[8, 9, 10, 11]	RMUSM	05/01/2001	0.53	14.43	14.64	0.57	6.06	15.94	11.64	6.17	6.96	6.14
Risk Managed - Global/International												
LVIP Global Equity Managed Volatility Fund - Service Class[1, 9, 10, 11]	RMGI	08/01/1985	0.69	6.54	6.82	2.99	1.89	12.38	11.84	6.21	7.82	6.85
LVIP State Street International Managed Volatility Fund - Service Class[1, 3, 9, 11]	RMGI	12/31/2013	0.11	11.84	12.84	1.83	3.49	20.06	14.44	5.96	5.98	3.28
ESG/Socially Conscious												
AB VPS Sustainable Global Thematic Portfolio - Class B[1]	ESC	01/11/1996	0.41	1.90	2.51	1.36	-1.22	0.73	5.90	-0.92	8.71	5.28
LVIP Nomura Social Awareness Fund - Service Class[9, 21]	ESC	05/02/1988	0.36	9.87	10.44	2.24	1.99	15.72	16.82	9.63	12.69	10.03

Printed on 09/03/2026 03:02PM ET

Performance Update

* These returns are measured from the inception date of the fund and predate its availability as an investment option in the variable annuity (separate account). This hypothetical representation depicts how the investment option would have performed had the fund been available in the variable annuity during the time period. It includes deductions for the M&E charge and the contract administrative fee. If selected above, the cost for the i4LIFE® Advantage feature or a death benefit will be reflected. The cost for other riders with quarterly charges is not reflected. No surrender charge and no annual contract charge is reflected.

Risk disclosure(s): The following summarizes some of the risks associated with the underlying funds available for investment. For risks specific to each investment option, please see each fund's prospectus.

1: **International**
Investing internationally involves risks not associated with investing solely in the United States, such as currency fluctuation, political or regulatory risk, currency exchange rate changes, differences in accounting and the limited availability of information.

2: **Asset Allocation Portfolios**
Asset allocation does not ensure a profit, nor protect against loss in a declining market.

3: **Fund of funds**
Each fund is operated as a fund of funds that invests primarily in one or more other funds, rather than in individual securities. A fund of this nature may be more expensive than other investment options because it has additional levels of expenses. From time to time, the Fund's advisor may modify the asset allocation to the underlying funds and may add new funds. A Fund's actual allocation may vary from the target strategic allocation at any point in time. Additionally, the Fund's advisor may directly manage assets of the underlying funds for a variety of purposes.

4: **Exchange-traded funds**
Exchange-traded funds (ETFs) in this lineup are available through collective trusts or mutual funds. Investors cannot invest directly in an ETF.

5: **Alternative Funds**
Certain funds (sometimes called "alternative funds") expect to invest in (or may invest in some) positions that emphasize alternative investment strategies and/or nontraditional asset classes and, as a result, are subject to the risk factors of those asset classes and/or investment strategies. Some of those risks may include general economic risk, geopolitical risk, commodity-price volatility, counterparty and settlement risk, currency risk, derivatives risk, emerging markets risk, foreign securities risk, high-yield bond exposure, index investing risk, exchange-traded notes risk, industry concentration risk, leveraging risk, real estate investment risk, master limited partnership risk, master limited partnership tax risk, energy infrastructure companies risk, sector risk, short sale risk, direct investment risk, hard assets sector risk, active trading and "overlay" risks, event-driven investing risk, global macro strategies risk, temporary defensive positions and large cash positions. If you are considering investing in alternative investment funds, you should ensure that you understand the complex investment strategies sometimes employed and be prepared to tolerate the risks of such asset classes. For a complete list of risks, as well as a discussion of risk and investment strategies, please refer to the fund's prospectus. The fund may invest in derivatives, including futures, options, forwards and swaps. Investments in derivatives may cause the fund's losses to be greater than if it invested only in conventional securities and can cause the fund to be more volatile. Derivatives involve risks different from, or possibly greater than, the risks associated with other investments. The fund's use of derivatives may cause the fund's investment returns to be impacted by the performance of securities the fund does not own and may result in the fund's total investment exposure exceeding the value of its portfolio.

6: **Target-date funds**
The target date is the approximate date when investors plan to retire or start withdrawing their money. Some target-date funds make no changes in asset allocation after the target date is reached; other target-date funds continue to make asset allocation changes following the target date. (See the prospectus for the funds allocation strategy.) The principal value is not guaranteed at any time, including at the target

Performance Update

date. An asset allocation strategy does not guarantee performance or protect against investment losses. A "fund of funds" may be more expensive than other types of investment options because it has additional levels of expenses.

7: **Emerging Markets**
Investing in emerging markets can be riskier than investing in well-established foreign markets. International investing involves special risks not found in domestic investing, including increased political, social and economic instability, all of which are magnified in emerging markets.

8: **Small & Mid Cap**
Funds that invest in small and/or midsize company stocks may be more volatile and involve greater risk, particularly in the short term, than those investing in larger, more established companies.

9: **Manager of managers funds**
Subject to approval of the fund's board, Lincoln Financial Investments Corporation (LFI) has the right to engage or terminate a subadvisor at any time, without a shareholder vote, based on an exemptive order from the Securities and Exchange Commission. LFI is responsible for overseeing all subadvisors for funds relying on this exemptive order.

10: **Multimanager**
For those LVIP funds that employ a multimanager structure, Lincoln Financial Investments Corporation (LFI) is responsible for overseeing the subadvisor(s). While the investment styles employed by the fund's subadvisors are intended to be complementary, they may not, in fact, be complementary, they may not, in fact, be complementary. A multimanager approach may result in more exposure to certain types of securities risks and in higher portfolio turnover.

11: **Managed Volatility Strategy**
The fund's managed volatility strategy is not a guarantee, and the fund's shareholders may experience losses. The fund employs hedging strategies designed to reduce overall portfolio volatility. The use of these hedging strategies may limit the upside participation of the fund in rising equity markets relative to unhedged funds, and the effectiveness of such strategies may be impacted during periods of rapid or extreme market events.

12: **Bonds**
The return of principal in bond funds is not guaranteed. Bond funds have the same interest rate, inflation, credit, duration, prepayment and market risks that are associated with the underlying bonds owned by the fund or account.

13: **Sector Funds**
Funds that target exposure to one region or industry may carry greater risk and higher volatility than more broadly diversified funds.

14: **REIT**
A real estate investment trust (REIT) involves risks such as refinancing, economic conditions in the real estate industry, declines in property values, dependency on real estate management, changes in property taxes, changes in interest rates and other risks associated with a portfolio that concentrates its investments in one sector or geographic region.

15: **Risk Management Strategy**
The fund's risk management strategy is not a guarantee, and the funds shareholders may experience losses. The fund employs hedging strategies designed to provide downside protection during sharp

Performance Update

downward movements in equity markets. The use of these hedging strategies may limit the upside participation of the fund in rising equity markets relative to other unhedged funds, and the effectiveness of such strategies may be impacted during periods of rapid or extreme market events.

16: **LVIP Government Money Market Fund**
You could lose money by investing in the Fund. Although the Fund seeks to preserve the value of your investment at $10.00 per share for LVIP Government Money Market Fund, it cannot guarantee it will do so. An investment in the Fund is not a bank account and is not insured or guaranteed by the Federal Deposit Insurance Corporation or any other government agency. The Fund's sponsor is not required to reimburse the Fund for losses, and you should not expect that the sponsor will provide financial support to the Fund at any time, including during periods of market stress.
The 7-day yield quotation more closely reflects the current earnings of the money market fund than the total return quotation.

17: **Macquarie Investment Management**
Investments in Macquarie VIP Series, Delaware Funds, Ivy Funds, LVIP Macquarie Funds or Lincoln Life accounts managed by Macquarie Investment Management Advisers, a series of Macquarie Investments Management Business Trust, are not and will not be deposits with or liabilities of Macquarie Bank Limited ABN 46008 583 542 and its holding companies, including their subsidiaries or related companies, and are subject to investment risk, including possible delays in prepayment and loss of income and capital invested. No Macquarie Group company guarantees or will guarantee the performance of the series or funds or accounts, the repayment of capital from the series or funds or account, or any particular rate of return.

18: **Ultra Short Bond Funds**
During periods of extremely low short-term interest rates, the fund may not be able to maintain a positive yield and, given a historically low interest rate environment, may experience risks associated with rising rates.

19: **Floating rate funds**
Floating rate funds should not be considered alternatives to CDs or money market funds and should not be considered as cash alternatives.

20: **High-yield or mortgage-backed funds**
High-yield funds may invest in high-yield or lower rated fixed income securities (junk bonds) or mortgage-backed securities with exposure to subprime mortgages, which may experience higher volatility and increased risk of nonpayment or default.

21: **ESG**
An environmental, social, governance (ESG) standards strategy (also referred to as engagement, green, impact, responsible, social aware, sustainable) generally prohibits investment in certain types of companies, industries and segments of the U.S. economy. Thus this strategy may (i) miss opportunities to invest in companies, industries or segments of the U.S. economy that are providing superior performance relative to the market as a whole and (ii) become invested in companies, industries and segments of the U.S. economy that are providing inferior performance relative to the market as a whole.

22: **Index**
An index is unmanaged, and one cannot invest directly in an index. Indices do not reflect the deduction of any fees.

23: **MSCI**
The fund described herein is indexed to an MSCI® index. It is not sponsored, endorsed, or promoted by MSCI®, and MSCI®; bears no liability with respect to any such fund or to an index on which a fund is based. The prospectus and statement of additional information contain a more detailed description of the limited relationship MSCI®; has with Lincoln Investment Advisors Corporation and any related funds.

Performance Update

24: S&P
The Index to which this fund is managed is a product of S&P Dow Jones Indices LLC (SPDJI) and has been licensed for use by one or more of the portfolio's service providers (licensee). Standard & Poor's®; and S&P®, S&P GSCI® and S&P 500® are registered trademarks of S&P Global, Inc. or its affiliates (S&P); Dow Jones® is a registered trademark of Dow Jones Trademark Holdings LLC (Dow Jones). The trademarks have been licensed for use by SPDJI and sublicensed for certain purposes by the licensee. The licensee's products are not sponsored, endorsed, sold or promoted by SPDJI, Dow Jones, S&P, their respective affiliates, or their third party licensors, and none of these parties or their respective affiliates or third party licensors make any representation regarding the advisability of investing in such products, nor do they have liability for any errors, omissions, or interruptions of the Index.

Important Disclosures
Variable products are issued by The Lincoln National Life Insurance Company, Fort Wayne, IN, distributed by Lincoln Financial Distributors, Inc., and offered by broker/dealers with an effective selling agreement. The Lincoln National Life Insurance Company is not authorized nor does it solicit business in the state of New York. **Contractual obligations are backed by the claims-paying ability of The Lincoln National Life Insurance Company.**
Limitations and exclusions may apply.
Lincoln Financial Group is the marketing name for Lincoln National Corporation and its affiliates. Affiliates are separately responsible for their own financial and contractual obligations.

Asset Categories

MCA	= Maximum Capital Appreciation
LTG	= Long Term Growth
GI	= Growth and Income
I	= Income
PC	= Preservation of Capital
RMAA	= Risk Managed - Asset Allocation
AsA	= Asset Allocation
RMUSL	= Risk Managed - US Large Cap
RMUSM	= Risk Managed - US Mid Cap
RMGI	= Risk Managed - Global/International
ESC	= ESG/Socially Conscious

AGENDA ITEM #12

(Closed Session)