VIRGINIA IT AGENCY

WELCOME TO THE

FEB. 2, 2022

ISOAG MEETING

VIRGINIA IT AGENCY

AGENDA

- WELCOME/INTRODUCTION: MIKE WATSON
- STEVE AIELLO/AHEAD
- NEDIM GOREN/NIST
- PATRICK ROBINSON/AT&T
- KATHY BORTLE & JAMES STURDEVANT/VITA
- UPCOMING EVENTS
- ADJOURN

Zero Trust According to NIST 800-207

Steven Aiello | Security and Compliance Director

Agenda

- Who am I and who is AHEAD?
- Zero Trust Principles
  - Zero Trust Definition
  - Tenants of Zero Trust
  - NIST 800-207 Anatomy of a Zero Trust
  - Zero Trust Deployment Approaches
- What do organizations miss with moving towards Zero Trust?
- Additional resources

AHEAD

AHEAD Security Overview

Security & Compliance Practice

AHEAD's Security Philosophy

"Security is a process, not a product"…

- The security industry has been overly focused on products.

Align security controls to proven threat actions

- Data clearly articulates the top TTPs that occur in over 99% of data breaches.

Build a program consisting of quality security processes

- There has been little focus on quality of outcomes in the security industry. Why do companies constantly pass audits, and constantly fail penetration tests?

What AHEAD Does for Customers

STRATEGY DEVELOPMENT

01

Building Strategy Together

AHEAD works with organizations to set strategy, internal stakeholders or teams to develop the strategy required

PROCESS ASSESSMENT & DEVELOPMENT

02

Building the Roadmap to Execution

AHEAD excels in translating security strategy into an executable process. Policy and standards creation are all critical functions when building the security program.

BUILD OPTIMIZATION

03

Executing the Plan for Success

Proper tool selection to reduce operational burden is critical to today's information security teams. Planning for security automation early eliminates repetitive work in the future.

OPERATIONS SUPPORT

04

Optimize Operations Cost and Overhead

Security automation is mission critical for modern I.T. environments. As operations team leverage orchestration and configuration management, security operations teams need to evolve their automation skills.

AHEAD

Zero Trust Principles

Building a Zero Trust Strategy

Zero Trust Definition According to NIS 800-207

“Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.”

Found on pg. 4 of NIST 800-207

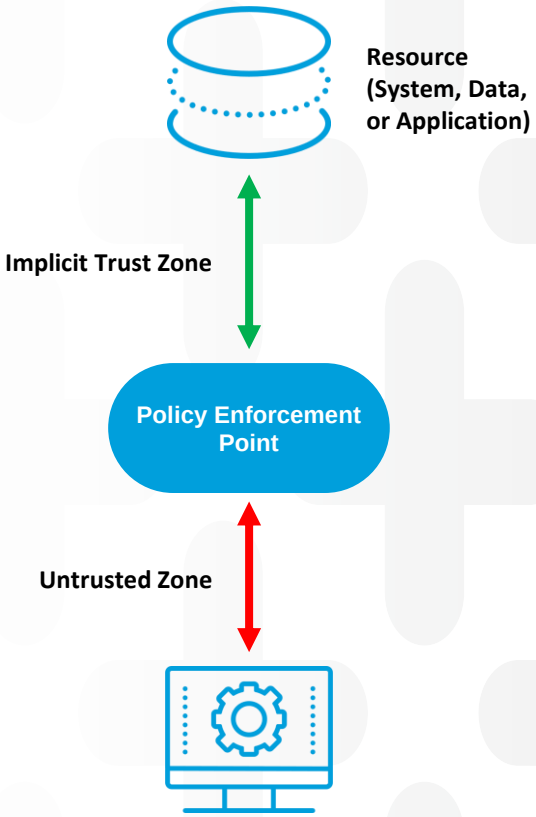
Tenets of Zero Trust

- All data sources and computing services are considered resources
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis
- Access to resources is determined by dynamic policy
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

Found on pg. 6 of NIST 800-207

Zero Trust Simplified

1. Zero Trust applies to two basic areas **authentication** and **authorization**.
2. What is the level of confidence unique request?
3. Is access to the resource allowable given the level of confidence in the subject's identity?
4. Does the device used for the request have the proper security posture?
5. Are there other factors that should be considered and that change the confidence level (e.g., time, location of subject, subject's security posture)?



Found on pg. 5 of NIST 800-207

NIST 800-207 Anatomy of a Zero Trust Architecture

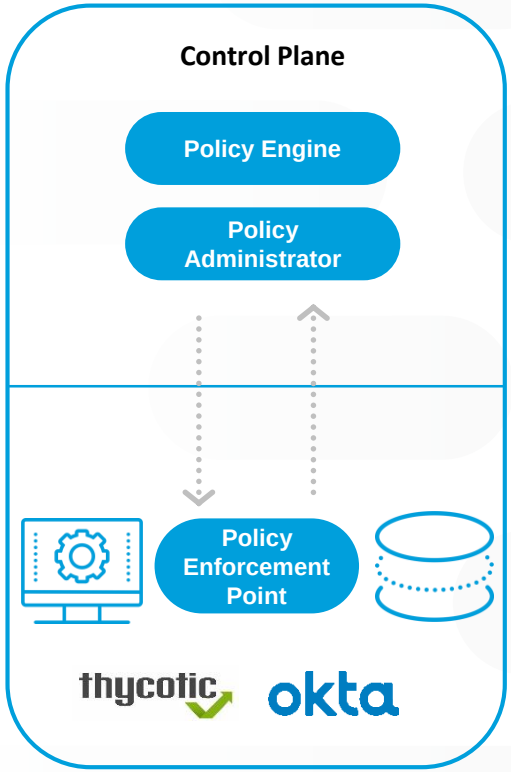
Any Trusted / Validated Device Granted Just in Time Access to Resources for an Authenticated User

Continuous diagnostics and mitigation **(CDM) system**. - gathers information about the enterprise asset's current state

Industry compliance system - This ensures that the enterprise remains compliant with any regulatory regime that it may fall under

Threat intelligence feed(s) - This provides information from internal or external sources that help the policy engine make access decisions.

Network and system activity logs - This enterprise system aggregates asset logs, network traffic, resource access actions, and other events that provide real-time feedback



You

Data Access Policies - These are the attributes, rules, and policies about access to enterprise resources

Public Key Infrastructure (PKI) - This system is responsible for generating and logging certificates issued by the enterprise to resources

ID Management System - This is responsible for creating, storing, and managing enterprise user accounts and identity records

Network Access / Policy Administrator

The Control and Data Plane

- **Policy Engine (PE):** This component is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from external sources as input to a trust algorithm

- **Policy Administrator (PA):** This component is responsible for establishing and/or shutting down the communication path between a subject and a resource

- **Policy Enforcement Point (PEP):** This system is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource

Four Zero Trust Deployment Approaches

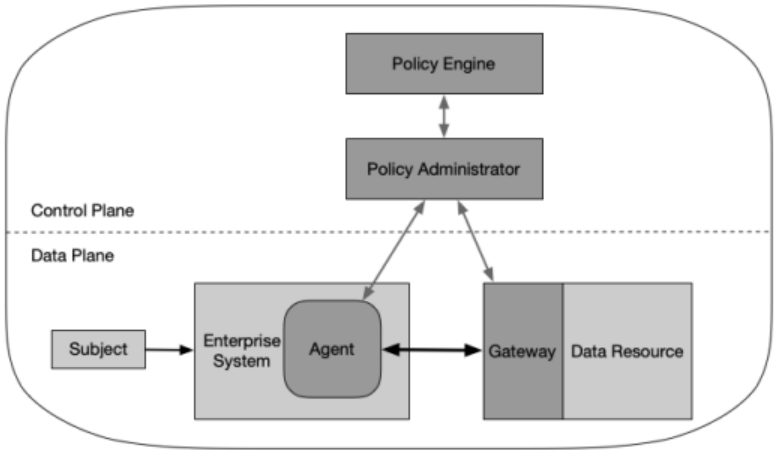


Figure 3: Device Agent/Gateway Model

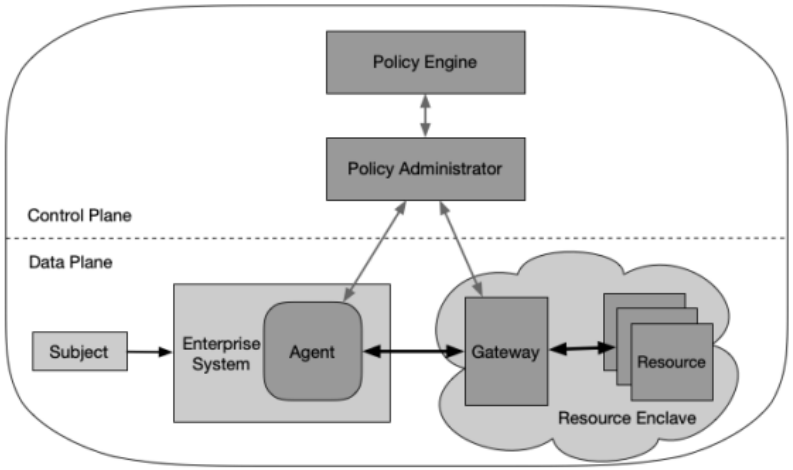


Figure 4: Enclave Gateway Model

In this deployment model, **the PEP is divided into two components that reside on the resource or as a component directly in front of a resource**. For example, each enterprise-issued asset has an installed device agent that coordinates connections, and each resource has a component (i.e., gateway) that is placed directly in front so that the resource communicates only with the gateway, essentially serving as a proxy for the resource

This deployment model is a variation of the device agent/gateway model above**. In this model, the gateway components may not reside on assets or in front of individual resources but instead reside at the boundary of a resource enclave**… these resources serve a single business function.

Four Zero Trust Deployment Approaches

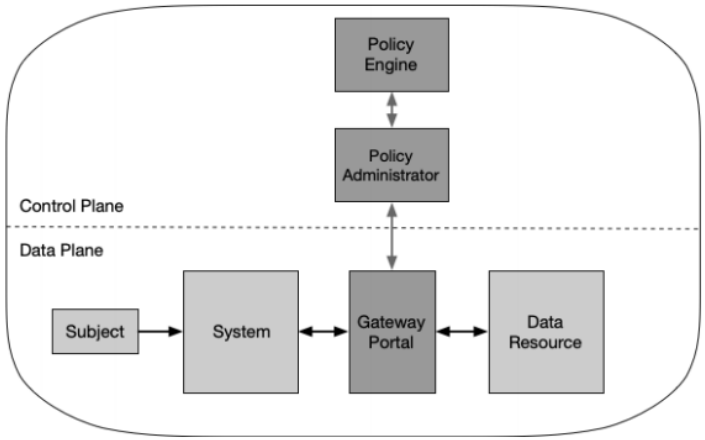


Figure 5: Resource Portal Model

This model is also more flexible for BYOD policies and interorganizational collaboration projects. Enterprise administrators do not need to ensure that each device has the appropriate device agent before use. However, limited information can be inferred from devices requesting access.

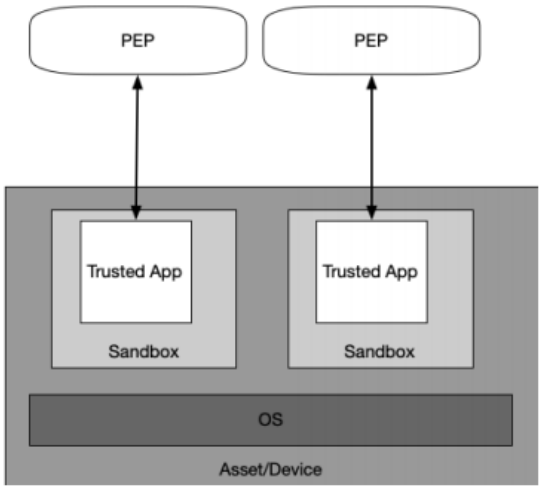


Figure 6: Application Sandboxes

Another variation of the agent/gateway deployment model is having vetted applications or processes run compartmentalized on assets. **These compartments could be virtual machines, containers, or some other implementation, but the goal is the same: to protect the application or instances of applications from a possibly compromised host** or other applications running on the asset

ZTA Using “Micro”-Segmentation

- An enterprise may choose to implement a ZTA based on placing individual or groups of resources on a unique network segment protected by a gateway security component.
- In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices to act as PEPs protecting each resource or small group of related resources. Alternatively (or additionally), the enterprise may choose to implement host-based micro-segmentation using software agents
- This approach requires an identity governance program (IGP) to fully function but relies on the gateway components to act as the PEP that shields resources from unauthorized access and/or discovery.

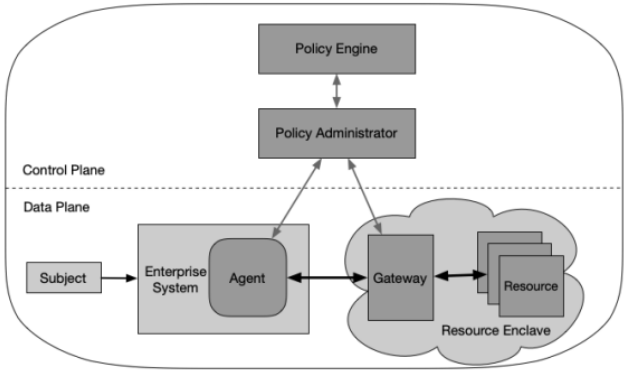


Figure 4: Enclave Gateway Model

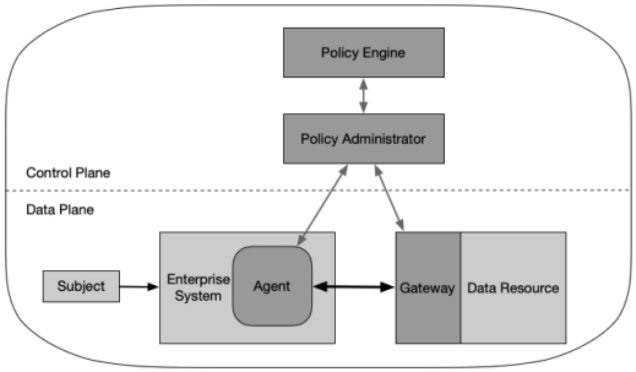


Figure 3: Device Agent/Gateway Model

ZTA Using Enhanced Identity Governance

- The enhanced identity governance approach to developing a ZTA uses the identity of actors as the key component of policy creation. Enhanced identity governance-based approaches for enterprises are often employed using an open network model or an enterprise network with visitor access or frequent non-enterprise devices on the network. Identity-driven approaches also work well for enterprises.
- that use cloud-based applications/services that may not allow for enterprise-owned or –operated ZT security components to be used

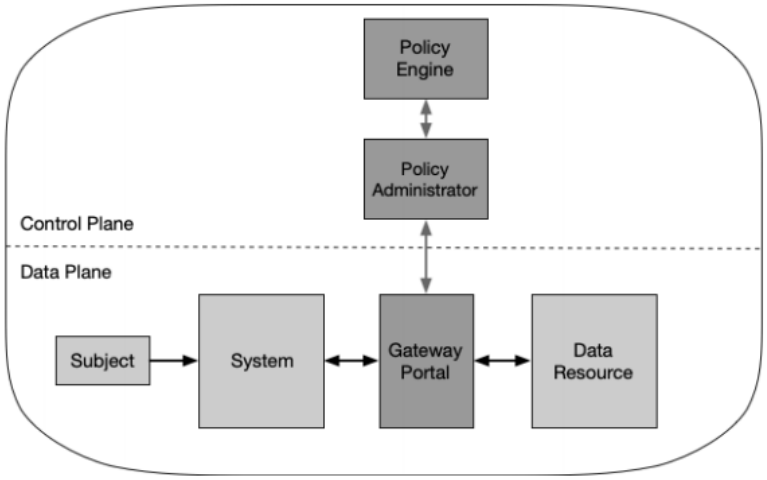


Figure 5: Resource Portal Model

AHEAD

What do Orgs Miss About Zero Trust?

Building a Zero Trust Strategy

What are Organizations Missing?

- Zero Trust Access Policy
  - The NIST 800-207 document touches on the fact that Zero Trust should be built on a defined access policy, however it does not provide guidance on how to create those policies.
- Backend Network Segmentation
  - Although organizations are making thinking about the access points into their applications, datacenter networks are still open and easy to navigate.
- Application Dependency Mappings
  - Organizations struggle with Application Dependency Mappings and don’t have clear visibility into how applications are interconnected.

AHEAD

Additional Zero Trust Reading

Google White Papers

https://cloud.google.com/beyondcorp/

- An overview: "A New Approach to Enterprise Security”
- How Google did it: "Design to Deployment at Google”
- Google's frontend infrastructure: "The Access Proxy”
- Migrating to BeyondCorp: "Maintaining Productivity while Improving Security”
- The human element: "The User Experience"
- Secure your endpoints: "Building a Healthy Fleet"

Thank You

AHEAD

Learn. Grow. Achieve.

thinkahead.com

nist.gov/rmf
sec-cert@nist.gov
nist.gov/social-media

What is New in NIST Special Publication 800-53A, Revision 5:

A brief summary of changes to NIST's control assessment guide

NIST SPECIAL PUBLICATION
SP 800-53A
53A
REVISION 5
ASSESSING SECURITY AND PRIVACY CONTROLS IN INFORMATION SYSTEMS AND ORGANIZATIONS
RISK MANAGEMENT FRAMEWORK

Briefing for:
Virginia Information Technologies Agency
Information Security Officers Advisory Group
February 2, 2022

Presented by:
Nedim Goren (NIST)
NIST Risk Management Framework (RMF) Project
(formerly NIST FISMA Implementation Project)

INFORMATION TECHNOLOGY LABORATORY
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

- NIST;
- Publication types & RMF publication ecosystem.

NIST Special Publication (SP) 800-53A, Revision 5

- Summary of changes in Revision 5;
- Specific changes in detail.

Public Comment Site

Q&A

Resources

Introduction

- RMF Team focus: Federal Information Security Modernization Act (FISMA) implementation and NIST Risk Management Framework (RMF);
- Risk Management vs. Compliance.

NIST mission:

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology *in ways that enhance economic security and improve our quality of life.*

National Institute of Standards and Technology
U.S. Department of Commerce

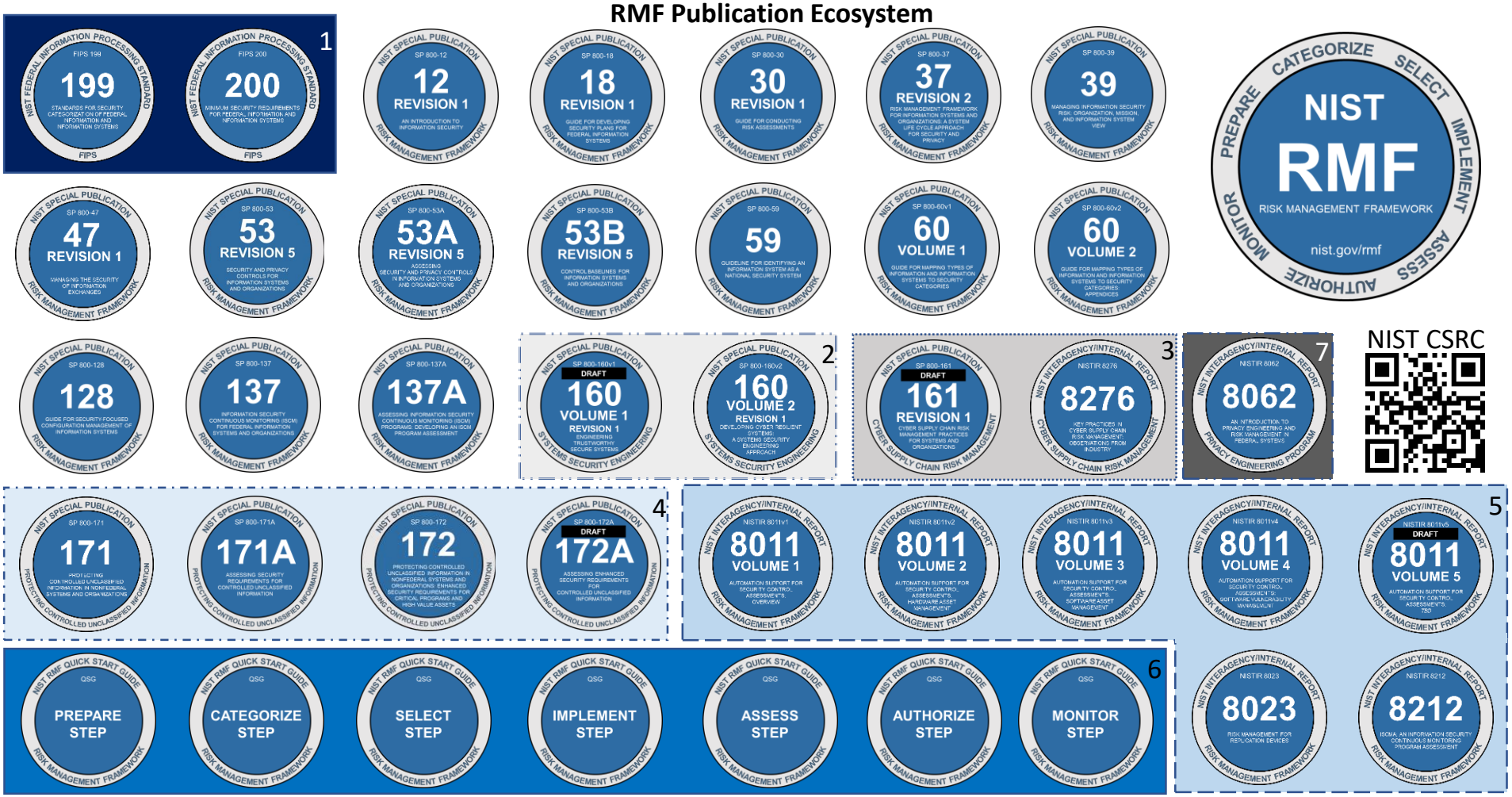
Publication Types

Federal Information Processing Standard (FIPS)
Special Publication (SP) • *SP 800 series: computer security* • *SP 1800 series: cybersecurity practice guides* • *SP 500 series: information technology*
NIST Interagency or Internal Report (NISTIR)
Other • NIST Handbooks • (NIST Information Technology Laboratory) Bulletins • White Papers • Guides (e.g., RMF Quick Start Guides) • Blog articles • Supplemental materials

NIST Computer Security Resource Center (CSRC)
https://csrc.nist.gov

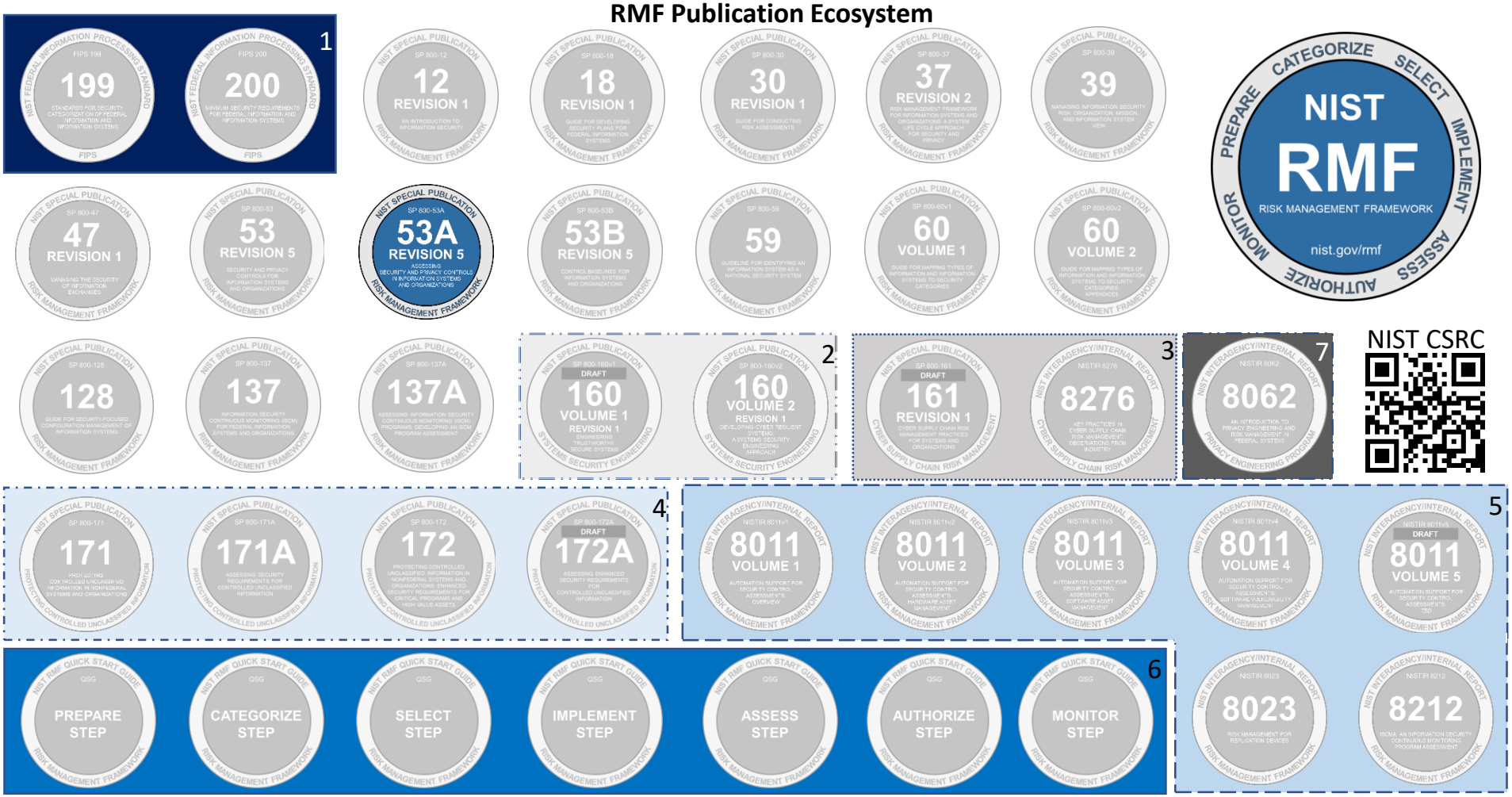
1-(All federal agencies) 2-Systems Security Engineering 3-Cyber Supply Chain Risk Management 4-Protecting Controlled Unclassified Information 5-RMF NISTIRs 6-RMF Quick Start Guides 7-Privacy Engineering Program

RMF Publication Ecosystem



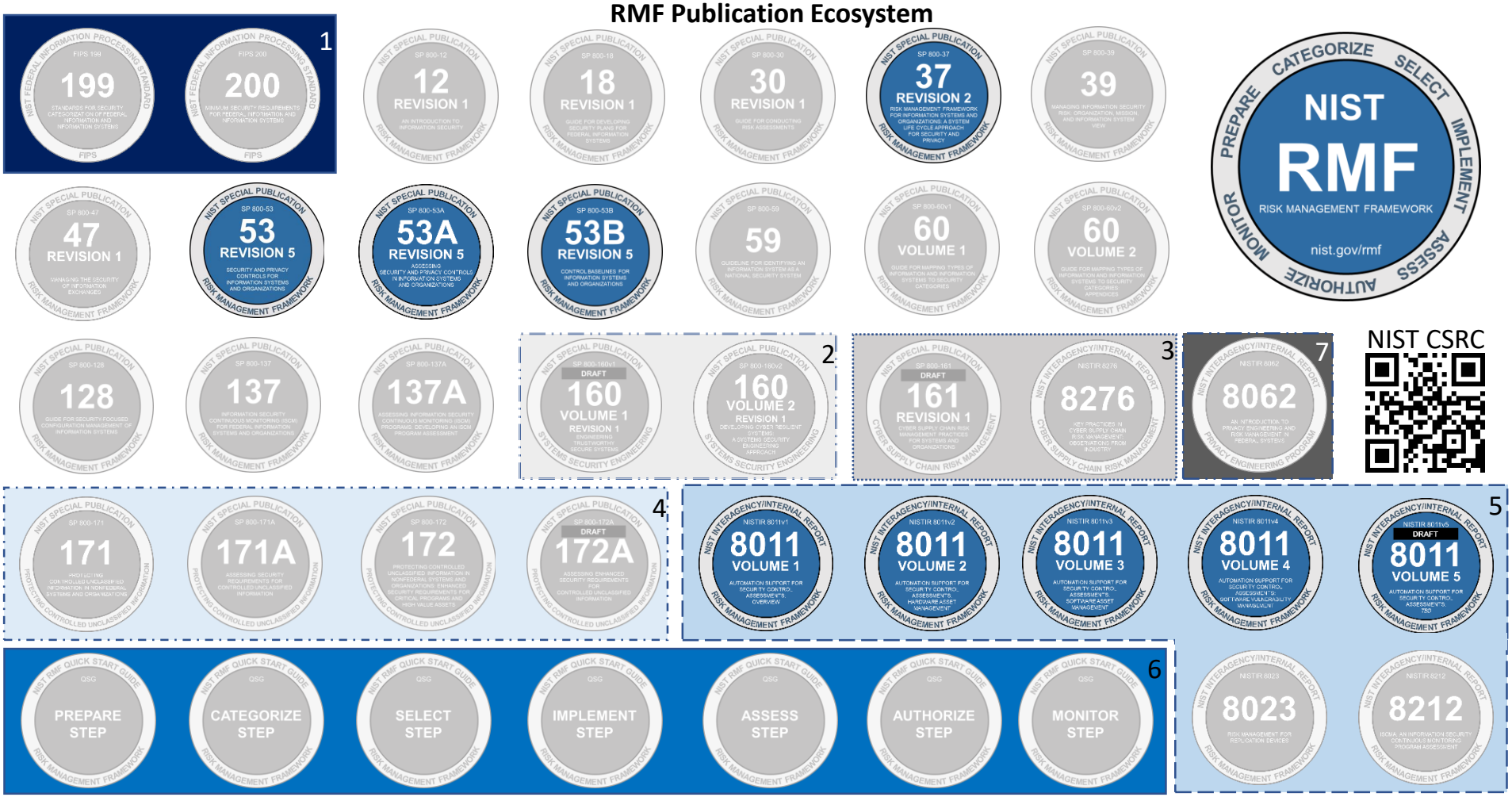
1-(All federal agencies) 2-Systems Security Engineering 3-Cyber Supply Chain Risk Management 4-Protecting Controlled Unclassified Information 5-RMF NISTIRs 6-RMF Quick Start Guides 7-Privacy Engineering Program

RMF Publication Ecosystem

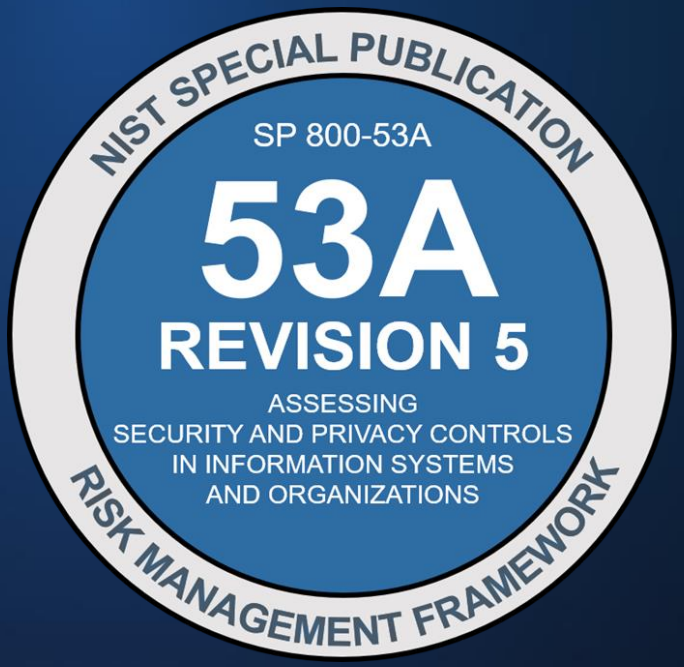


1-(All federal agencies) 2-Systems Security Engineering 3-Cyber Supply Chain Risk Management 4-Protecting Controlled Unclassified Information 5-RMF NISTIRs 6-RMF Quick Start Guides 7-Privacy Engineering Program

RMF Publication Ecosystem



National Institute of Standards and Technology
U.S. Department of Commerce



Overview: SP 800-53A Revision 5

Purpose: To facilitate (SP 800-53) control assessments within an effective risk management framework.

Publication organized in two major parts:

1. Process to conduct effective control assessments (*Prepare, Develop Plans, Conduct Assessments, Analyze Results*) → "front matter";
2. (Initial) assessment procedures that correspond with SP 800-53, Revision 5 controls.

SP 800-53 control assessments:

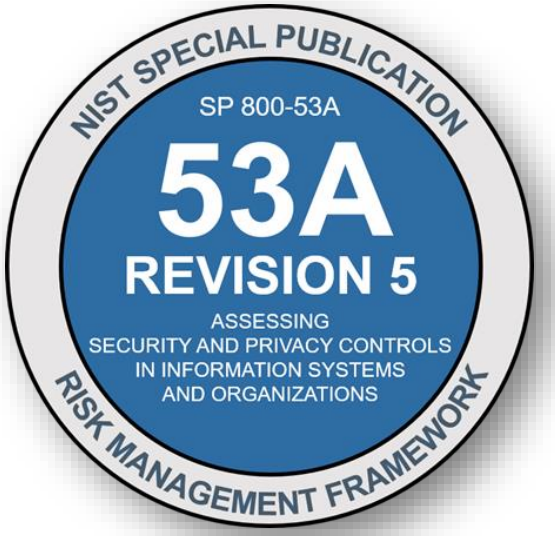
- ☑ Determine overall effectiveness of implemented controls;
- ☑ Provide indication of quality of risk management process;
- ☑ Inform security & privacy strengths/weaknesses of the system/organization.

- ⊘ Not a checklist;
- ⊘ Not a simple pass/fail audit;
- ⊘ Not a paperwork exercise to pass inspections/audits.

NIST SP 800-53A

SP 800-53A, Revision 5 includes:

- Updated assessment procedures to correspond with SP 800-53, Revision 5 controls;
- New assessment procedure structure to:
  - Improve the efficiency of conducting control assessments;
  - Provide better traceability between assessment procedures & controls;
  - Better support the use of automated tools, continuous monitoring, and ongoing authorization programs.
- Assessment procedures in PDF, CSV, plain text, and OSCAL (XML, YAML, JSON) formats.



33

Control Assessment Process

Repeatable process to ***prepare*** for, ***develop plans*** for, and ***conduct*** control assessments, and ***analyze*** assessment results

Each step (*Prepare, Develop, Conduct, Analyze*) includes:

- ***Purpose;***
- ***Primary Roles;***
- ***Outcomes;***
- ***In-depth Tasks.***

Sample SP 800-53A Assessment Procedure:

SP 800-53A Rev 4 (2014)

AC-16	SECURITY ATTRIBUTES			
	ASSESSMENT OBJECTIVE: *Determine if the organization:*			
	AC-16(a)	AC-16(a)[1]	*defines types of security attributes to be associated with information:*	
			AC-16(a)[1][a]	*in storage;*
			AC-16(a)[1][b]	*in process; and/or*
			AC-16(a)[1][c]	*in transmission;*
		AC-16(a)[2]	*defines security attribute values for organization-defined types of security attributes;*	
		AC-16(a)[3]	*provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information:*	
			AC-16(a)[3][a]	*in storage;*
			AC-16(a)[3][b]	*in process; and/or*
			AC-16(a)[3][c]	*in transmission;*
	AC-16(b)	*ensures that the security attribute associations are made and retained with the information;*		
	AC-16(c)	AC-16(c)[1]	*defines information systems for which the permitted organization-defined security attributes are to be established;*	
		AC-16(c)[2]	*defines security attributes that are permitted for organization-defined information systems;*	
		AC-16(c)[3]	*establishes the permitted organization-defined security attributes for organization-defined information systems;*	
	AC-16(d)	AC-16(d)[1]	*defines values or ranges for each of the established security attributes; and*	
		AC-16(d)[2]	*determines the permitted organization-defined values or ranges for each of the established security attributes.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:			
	Examine: [*SELECT FROM:* Access control policy; procedures addressing the association of security attributes to information in storage, in process, and in transmission; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].			
	Interview: [*SELECT FROM:* System/network administrators; organizational personnel with information security responsibilities; system developers].			
	Test: [*SELECT FROM:* Organizational capability supporting and maintaining the association of security attributes to information in storage, in process, and in transmission].			

SP 800-53A Rev 5 (2022)

AC-16	SECURITY AND PRIVACY ATTRIBUTES	
	ASSESSMENT OBJECTIVE *Determine if:*	
	AC-16_ODP[01]	*types of security attributes to be associated with information security attribute values for information in storage, in process, and/or in transmission are defined;*
	AC-16_ODP[02]	*types of privacy attributes to be associated with privacy attribute values for information in storage, in process, and/or in transmission are defined;*
	AC-16_ODP[03]	*security attribute values for types of security attributes are defined;*
	AC-16_ODP[04]	*privacy attribute values for types of privacy attributes are defined;*
	AC-16_ODP[05]	*systems for which permitted security attributes are to be established are defined;*
	AC-16_ODP[06]	*systems for which permitted privacy attributes are to be established are defined;*
	AC-16_ODP[07]	*security attributes defined as part of AC-16a that are permitted for systems are defined;*
	AC-16_ODP[08]	*privacy attributes defined as part of AC-16a that are permitted for systems are defined;*
	AC-16_ODP[09]	*attribute values or ranges for established attributes are defined;*
	AC-16_ODP[10]	*the frequency at which to review security attributes for applicability is defined;*
	AC-16_ODP[11]	*the frequency at which to review privacy attributes for applicability is defined;*
	AC-16a.[01]	*the means to associate <AC-16_ODP[01] types of security attributes> with <AC-16_ODP[03] security attribute values> for information in storage, in process, and/or in transmission are provided;*
	AC-16a.[02]	*the means to associate <AC-16_ODP[02] types of privacy attributes> with <AC-16_ODP[04] privacy attribute values> for information in storage, in process, and/or in transmission are provided;*
	AC-16b.[01]	*attribute associations are made;*
	AC-16b.[02]	*attribute associations are retained with the information;*
	AC-16c.[01]	*the following permitted security attributes are established from the attributes defined in AC-16a. for <AC-16_ODP[05] systems>: <AC-16_ODP[07] security attributes>;*
	AC-16c.[02]	*the following permitted privacy attributes are established from the attributes defined in AC-16a. for <AC-16_ODP[06] systems>: <AC-16_ODP[08] privacy attributes>;*
	AC-16d.	*the following permitted attribute values or ranges for each of the established attributes are determined: <AC-16_ODP[09] attribute values or ranges>;*
	AC-16e.	*changes to attributes are audited;*
	AC-16f.[01]	*<AC-16_ODP[07] security attributes> are reviewed for applicability <AC-16_ODP[10] frequency>;*
	AC-16f.[02]	*<AC-16_ODP[08] privacy attributes> are reviewed for applicability <AC-16_ODP[11] frequency>.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16 Examine	*[SELECT FROM: Access control policy; procedures addressing the association of security and privacy attributes to information in storage, in process, and in transmission; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].*
	AC-16 Interview	*[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers].*
	AC-16 Test	*[SELECT FROM Organizational capability supporting and maintaining the association of security and privacy attributes to information in storage, in process, and in transmission].*

SP 800-53 and SP 800-53A

NIST SPECIAL PUBLICATION
SP 800-53
53
REVISION 5
SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS
RISK MANAGEMENT FRAMEWORK

AC-17 REMOTE ACCESS

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

Discussion: Remote access is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless. Organizations use encrypted virtual private networks

NIST SPECIAL PUBLICATION
SP 800-53A
53A
REVISION 5
ASSESSING SECURITY AND PRIVACY CONTROLS IN INFORMATION SYSTEMS AND ORGANIZATIONS
RISK MANAGEMENT FRAMEWORK

AC-17	REMOTE ACCESS	
	ASSESSMENT OBJECTIVE *Determine if:*	
	AC-17a.[01]	*usage restrictions are established and documented for each type of remote access allowed;*
	AC-17a.[02]	*configuration/connection requirements are established and documented for each type of remote access allowed;*
	AC-17a.[03]	*implementation guidance is established and documented for each type of remote access allowed;*
	AC-17b.	*each type of remote access to the system is authorized prior to allowing such connections.*

SP 800-53A Revision 5 Assessment

Assessment Objectives

Bracketed numbers indicates granularization from the SP 800-53 control item.

Corresponds directly with SP 800-53 control item

Potential Methods & Objects

NEW Control ID "Tag" for Potential Methods

AC-17	REMOTE ACCESS
	ASSESSMENT OBJECTIVE *Determine if:*
AC-17a.[01]	*usage restrictions are established and documented for each type of remote access allowed;*
AC-17a.[02]	*configuration/connection requirements are established and documented for each type of remote access allowed;*
AC-17a.[03]	*implementation guidance is established and documented for each type of remote access allowed;*
AC-17b.	*each type of remote access to the system is authorized prior to allowing such connections.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
AC-17-Examine	*[SELECT FROM: Access control policy; procedures addressing remote access implementation and usage (including restrictions); configuration management plan; system configuration settings and associated documentation; remote access authorizations; system audit records; system security plan; other relevant documents or records].*
AC-17-Interview	*[SELECT FROM: Organizational personnel with responsibilities for managing remote access connections; system/network administrators; organizational personnel with information security responsibilities].*
AC-17-Test	*[SELECT FROM: Remote access management capability for the system].*

SP 800-53A Revision 5 Assessment Procedure Schema:

NEW Organization-defined Parameters "unique ID"

CM-02	BASELINE CONFIGURATION
	ASSESSMENT OBJECTIVE *Determine if:*
CM-02_ODP[01]	***the frequency of baseline configuration review and update is defined;***
CM-02_ODP[02]	***the circumstances requiring baseline configuration review and update are defined;***
CM-02a.[01]	*a current baseline configuration of t system is developed and documented;*
CM-02a.[02]	on
CM-02b.01	*the baseline configuration of the system is reviewed and updated <CM-02_ODP[01] frequency>;*
CM-02b.02	*the baseline configuration of the system is reviewed and updated when ed due to <CM-02_ODP[02] circumstances>;*
CM-02b.03	*the baseline configuration of the system is reviewed a components are installed or upgraded.*
POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
CM-02-Examine	*[SELECT FROM: Configuration management policy; pro configuration of the system; configuration management plan; enterprise architecture documentation; system design documentation; system security plan; privacy plan; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; change control records; other relevant documents or records]*

NEW Schema for Defining Organization-Defined Parameter

Assignment Statements

ODP "unique ID" followed by short phrase to describe the ODP that was previously defined

SP 800-53A Revision 5 Assessment Procedure Schema:

NEW Schema for Defining Organization-Defined Parameter ***Selection Statements***

AC-02(02)	ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT
	ASSESSMENT OBJECTIVE: *Determine if:*
AC-02(02)_ODP[01]	***one of the following PARAMETER VALUES is selected: {remove; disable};***
AC-02(02)_ODP[02]	***the time period after which to automatically remove or disable temporary or emergency accounts is defined;***
AC-02(02)	temporary and emergency accounts are automatically ***<AC-02(02)_ODP[01] SELECTED PARAMETER VALUE***> after ***<AC-02(02)_ODP[02] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
AC-02(02)-Examine	[SELECT FROM: Access control policy; proce management; system design documentatio and associated documentation; system-ger removed and/or disabled; system-generate removed and/or disabled; system audit records; system security plan; other relevant documents or records].
AC-02(02)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security with information security responsibilities; system developers].
AC-02(02)-Test	[SELECT FROM: Automated mechanisms for implementing account management functions].

ODP "unique ID" followed by SELECTED PARAMETER

SP 800-53A Revision 5 Assessment Procedure Schema: nested ODPs in selection operations

RA-05(02)	VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE
	ASSESSMENT OBJECTIVE
	Determine if:
	RA-05(02)_ODP[01] — ***one or more of the following PARAMETERS is/are selected: {<RA-05(02)_ODP[02] frequency>; prior to a new scan; when new vulnerabilities are identified and reported};***
	RA-05(02)_ODP[02] — ***the frequency for updating the system vulnerabilities scanned is defined (if selected);***
	RA-05(02) — *the system vulnerabilities to be scanned are updated <RA-05(02)_ODP[01] SELECTED PARAMETER(S)>.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
	RA-05 — *addressing vulnerability scanning; assessment report; vulnerability scanning tools; on documentation; vulnerability; em security plan; other relevant*
	RA-05 — *onal personnel with vulnerability; sonnel with vulnerability scan analysis responsibilities; organizatio system/network administrators].*
	RA-05(02)-Test — *[SELECT FROM: Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning].*

NEW Schema for Defining Organization-Defined Parameter ***Selection Statements***

NEW Schema for embedded ***Assignment Statement*** within a selection statement

NEW Schema for ***Selection Statement*** in the Assessment Objective

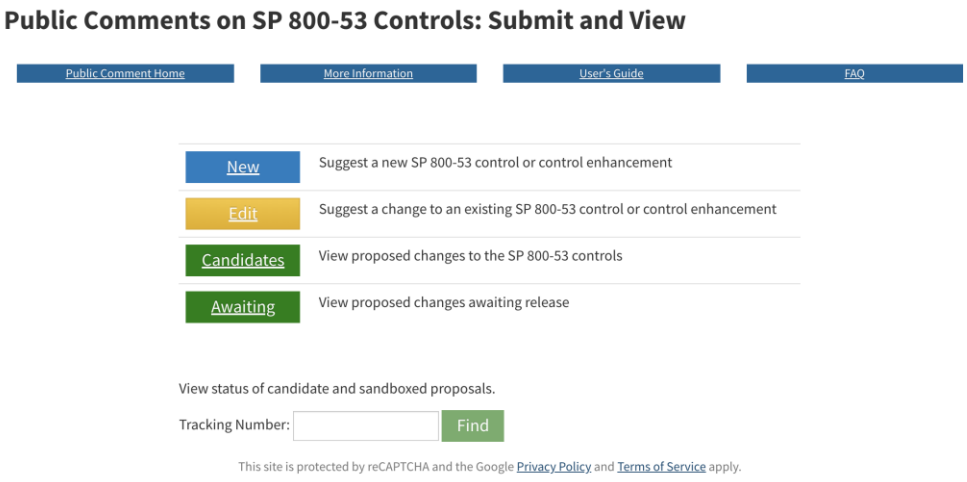
800-53 PUBLIC COMMENT SITE

SP 800-53

53

SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

nist.gov/rmf/sp800-53-controls



Preview new/updated controls and control enhancements to be included in next revision

SP 800-53 controls, baselines, and assessment procedures* as a **machine-readable & web-based data set**

Bi-annual **minor updates***

Major updates* every 2 years

Allows for public comment and review – suggest edits to current controls and comment on others' comments

NIST will continue to accept comments on SP 800-53 via comment matrix submitted by email.

Receive status updates when a comment is reviewed by NIST, published as draft for public comment, or included in a revision

Enables stakeholders to:

- Comment on (final) controls at any time;
- During public comment periods, focus on controls with proposed changes;
- Preview controls awaiting publication (in next revision);

Better plan for & allocate resources to giving feedback & implementing updates

- See the status of a submitted comment.

Increase transparency

Enables NIST to:

- Solicit more specific & actionable feedback;
- Maintain & issue an up-to-date controls;
- Release SP 800-53 in multiple data formats;
- Promote use of automation.

Deliver a more dynamic, up-to-date & useable control catalog

National Institute of Standards and Technology
U.S. Department of Commerce

nist.gov/rmf sec-cert@nist.gov nist.gov/social-media

Resources

Resources

NIST Risk Management Framework (RMF) website
https://nist.gov/rmf

General Mailbox
sec-cert@nist.gov

RMF Online Course (free 3-hour, on-demand, self-paced, no registration required)
https://csrc.nist.gov/Projects/risk-management/rmf-training

NIST Cybersecurity Program Overview
https://nist.gov/cyber

NIST Technical Series Publications
https://www.nist.gov/nist-research-library/nist-publications

NIST Cybersecurity Publications
https://csrc.nist.gov

Resources

Computer Security Resource Center (CSRC) email updates
https://public.govdelivery.com/accounts/USNIST/subscriber/new?qsp=USNIST_3

NIST Risk Management Framework (RMF) (FISMA Implementation) Project Mailing List (announce list)
https://csrc.nist.gov/Projects/risk-management/mailing-list

Drafts Open for Comment
https://csrc.nist.gov/publications/drafts-open-for-comment

NIST Security and Privacy Control Overlay Repository (SCOR)
https://csrc.nist.gov/Projects/Risk-Management/scor

NIST National Cybersecurity Center of Excellence (NCCoE)
https://www.nccoe.nist.gov

NIST SP 800-53 Control and Control Baseline Release Search Site + Public Comment Site
https://nist.gov/rmf/sp800-53-controls

AT&T

CYBERSECURITY AND ZERO TRUST STRATEGY

VIRGINIA IT AGENCY

AT&T Business

NASCIO 2022 Top Priorities

STATE CIO TOP 10 PRIORITIES

2022 Strategies, Policy Issues and Management Processes

1
Cybersecurity and Risk Management: governance; budget and resource requirements; security frameworks; data protection; training and awareness; insider threats; third party risk

2
Digital Government / Digital Services: framework for digital services; portal; improving and digitizing citizen experience; accessibility; identity management; digital assistants; privacy

3
Broadband / Wireless Connectivity: strengthening statewide connectivity; implementing rural broadband expansion; 5G deployment

4
Cloud Services: cloud strategy; selection of service and deployment models; scalable and elastic services; governance; service management; security; privacy; procurement

5
Legacy Modernization: enhancing, renovating, replacing, legacy platforms and applications; business process improvement

6
Identity and Access Management: supporting citizen digital services; workforce access; access control; authentication; credentialing; digital standards

7
Workforce: preparing for the future workforce and reimagining the government workforce; transformation of knowledge, skills and experience; more defined roles for IT asset management, business relationship management skills, service integration

8
Enterprise Architecture: governance; formulating, refining or implementing an EA strategy; business architecture; business process modeling; statewide EA program management; federal reference models; whole-government enterprise architecture

9
Data and Information Management: data governance; data architecture; master data management; open data; sustained access to government data; data portals; enhancing the role of data; information & intelligence, knowledge management; data integration; data management strategy; roles and responsibilities; dataops

10
Consolidation/Optimization: centralizing; consolidating services; operations; resources; infrastructure; data centers; communications and marketing "enterprise" thinking

5G MEC AND ZERO TRUST

5G

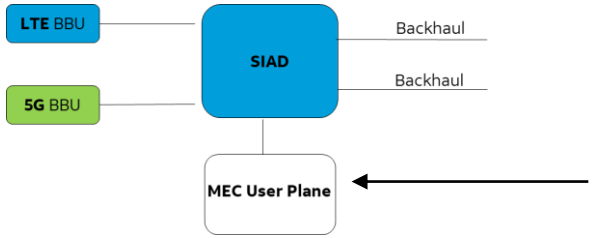
- DoD has invested heavily in standing up 5G testbeds through Tranche 1 & 2 OTA's
  - AT&T has received multiple awards on these, including the Navy Warehouse, Army JBLM, and Nellis AF Base
- Innovation brought to these projects include dedicated, multi-operator core network (MOCN) 5G
  - A private 5G core deployed for DoD, combined with AT&T commercial core
  - Provides DoD benefits of private with resiliency and backup of AT&T commercial
- In addition to 5G native capabilities, AT&T security innovation brought to these projects include
  - Micro segmentation
  - IDAM
  - SIEM Analytics
  - Localized Security VM's on MEC

5G

FIRSTNET™ Built with AT&T

MEC

- Traditional cellular traffic flows require control and user plane traffic to stay together
- As applications and security moves to the edge, this creates a hairpin flow of user plane traffic that introduces performance degradation
- MEC enables Control User Plane Traffic Separation (CUPS)
  - Enables user plane data to stay local for applications at the edge
- MEC server enables cloud compute and security functions to be placed at the edge
  - Decreased latency for intensive applications such as AR/VR



Applications and Security Functions Stay local

OVERVIEW OF AT&T THREAT INSIGHTS SERVICE

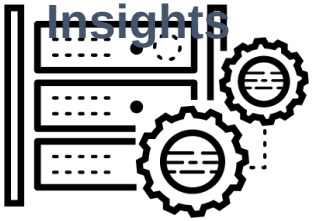
AT&T Internet Sensor Grid

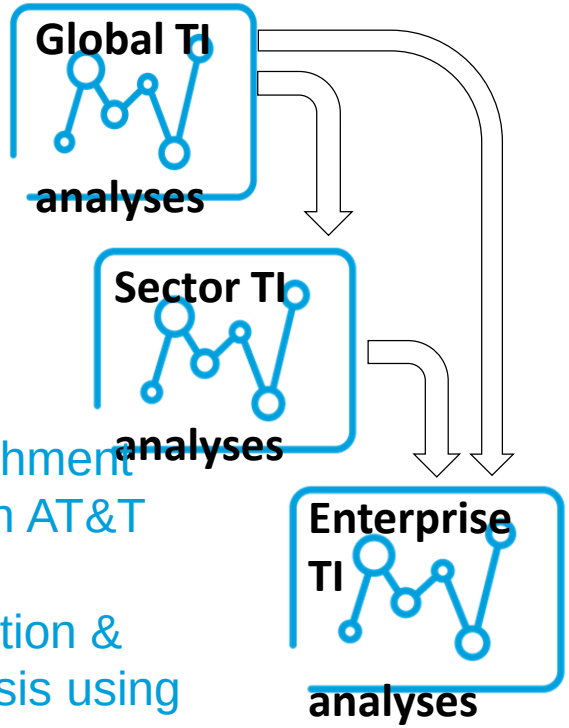
Trillions Global Internet Flow and DNS records

Billions Sector Internet Flow and DNS records

Millions Enterprise Internet Flow and DNS records

Threat Insights





Goal: Detect and alert on threats as early as possible in attack life-cycle to remediate and even prevent damage.

- Metadata enrichment
- Correlation with AT&T threat intel
- Anomaly detection & behavior analysis using AI/ML methods
- Automated alert delivery
- Global & Sector analyses informs Enterprise analyses

EXAMPLE THREAT INSIGHTS: LOG4J EARLY WARNINGS

Prior to Log4j awareness, Threat Insights had already detected 52 of the threat IPs
Another 46 by AT&T threat intel, for a total of 266 IPs in Threat Insights before Log4j

Early warning that the vulnerability began to be exploited in Threat Insights CVE alerts:

1. 20211210 0300 EST: CVE-2021-44228 Apache Log4j JAVA Naming and Directory Interface (JNDI) vulnerability
2. 20211214 1530 EST: CVE-2021-45046 Incomplete fix to CVE-2021-44228 allows RCE
3. 20211218 0530 EST: CVE-2021-45105 Uncontrolled recursion in Apache Log4j2
4. 20211228 1445 EST: CVE-2021-44832 JDBC appender RCE vulnerability in Apache Log4j2

FEDERAL AGENCY USE CASE: LOG4J

1. First-stage: 2-way content web/DNS flows

    Log4j attacks web or DNS servers

    Agency serves web or DNS responses

Found:

    Exploitation prior to public awareness

    Most inbound traffic from log4j came from RU

    Highest outbound to 2 RU threat actors

2. Second-stage: 2-way content flows LDAP/RMI

    Agency initiates LDAP request

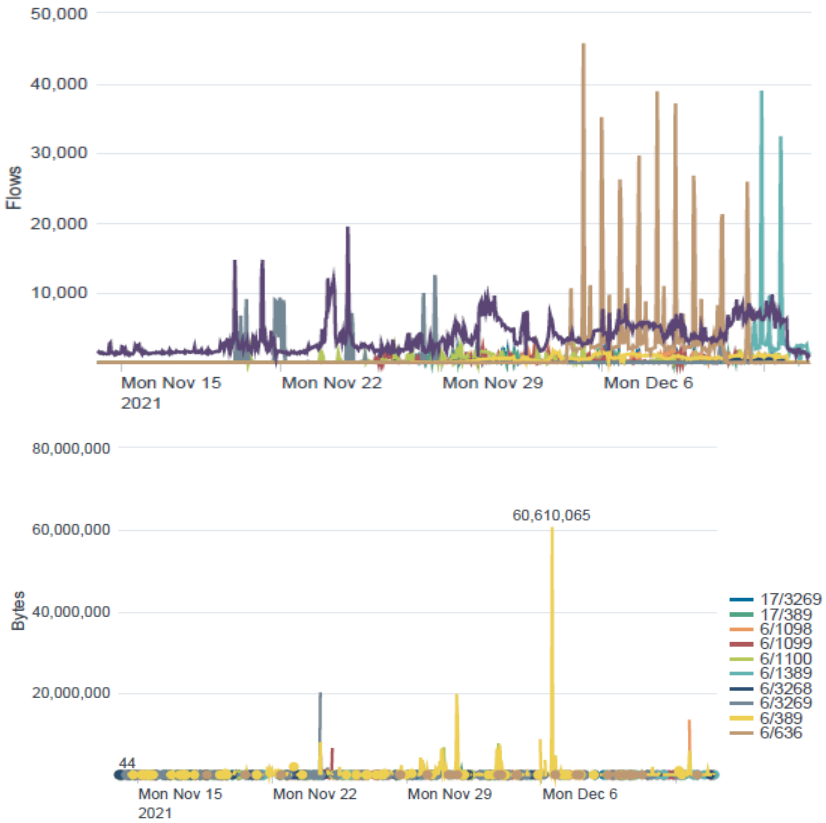
    Potentially compromised LDAP server response

Found:

    Outbound UDP/389 LDAP spike to single IP, 60+M bytes

    Outbound TCP/3268 to Threat Insights IOC IP with high BPP= 1060, 36 second flows, 6.7M bytes

    Outbound TCP/636 to 354 threat actors known to Threat Insights



AT&T Business

VIRGINIA IT AGENCY

VITA/CSRM PHISHING SERVICE

KATHY BORTLE & JAMES STURDEVANT, SR.

Incident Response Specialists

VITA/CSRM/THREAT MANAGEMENT TEAM

OCT. 6, 2022

VIRGINIA IT AGENCY

VITA/CSRM PHISHING SERVICE

KATHY BORTLE & JAMES STURDEVANT, SR.

Incident Response Specialists

VITA/CSRM/THREAT MANAGEMENT TEAM

OCT. 6, 2022

BACKGROUND

BACKGROUND

- VITA started hosting phishing campaigns to assist agencies with training their users on how to recognize a phishing message in a safe controlled environment.
- At the time, VITA had purchased an add-on option to Metasploit to handle the campaigns. While the tool was very flexible, the reporting was rather lacking. If multiple agencies were phished at the same time, all results would have to be manually reviewed and correlated to provide user data to each agency. This was a very time consuming task and limited the number of campaigns that could be done in a year.
- Due to the increase in ransomware attacks, the Virginia Legislature directed VITA to perform phishing campaigns across the Commonwealth and provided a budget for the tools for six years.
- VITA evaluated multiple phishing tools and decided to purchase the SANS phishing tool. It is much easier to use and allows flexibility in reporting results.

MEETING SECURITY REQUIREMENTS

REQUIREMENTS

- VITA has 33,000 phishing (as of Jan. 30, 2022, 6,000 have been used) licenses a year to phish the Commonwealth's approximate 65,000 users.
- In order for agencies to maintain compliance with SEC 525, the VITA/CSRM/Threat Management Team will phish half of the agency each year.
- Example: If an agency has 500 users, they would be able to phish 250 users years one, three and 5, and the other 250 users years two, four and six.
- Agencies will need to provide VITA/CSRM with the names of employees that they want to phish that year. Once an employee has been assigned a phishing license, they can be phished multiple times during the year.
- At the end of the two-year cycle, all employees should have been phished at least once.

HOW TO GET STARTED

STEPS TO CREATE A PHISHING CAMPAIGN

1. Send an email with your contact information to Commonwealth Security requesting a phishing campaign.

   Email: CommonwealthSecurity@vita.Virginia.gov

2. The VITA/CSRM/Threat Management Team will reach out to you to discuss developing the campaign.

3. The first step will be to create a template for the campaign. You will discuss what you want the phishing message to look like – type of industry, recent news topics, has an attachment, has links for filling out forms, etc.

4. The team will take this information and develop a template for the campaign.

5. Once the template is created, they will send sample phish messages to you so that you can see what it will look like and how it will work.

6. After a final version of the template is agreed, we are ready to setup the campaign and schedule it.

STEPS TO CREATE A PHISHING CAMPAIGN (CONT.)

7. To setup the campaign, the team will need to know the following:
    - First and last names of the users to be phished;
    - Email addresses of the users to be phished;
    - How long do you want the campaign to run (max is normally three days);
    - When do you want the campaign to start (date/time);
    - When do you want the campaign to run (hours, days, etc.).
8. The Threat Management team will use this information to setup the campaign and let you know when it is ready.
9. The campaign will be launched at the agreed date/time.
10. When the campaign is finished, the threat management team will pull the campaign results and provide it to you for review.
11. If you wish to re-test your users or run additional campaigns, please return to step one of the process by sending another email to Commonwealth Security.

CONTACT INFO

Dean Johnson, Director of Threat Management

Dean.Johnson@vita.Virginia.gov

804-416-8785

Kathy Bortle , Incident Response Specialist

Kathy.Bortle@vita.Virginia.gov

804-416-6061

Jim Sturdevant, Sr., Incident Response Specialist

Jim.Sturdevant@vita.Virginia.gov

804-416-6038

VIRGINIA IT AGENCY

Upcoming events

CYBERSECURITY AWARENESS TRAINING COMPLIANCE VERIFICATION FORM

1. This form should have been completed and submitted by Jan. 31, 2022.
2. The form maybe completed manually or in Archer. In Archer, click on the “Verification and Compliance Tab” under the Security Awareness Training Questionnaire. If you do not see the tab, click on recalculate and it should appear.
3. If you have not submitted your form, please do so as soon as possible.

Appendix II

Annual Cybersecurity Awareness Training Verification
Compliance Form

In accordance with the Code of Virginia, Section 2.2-2009 sub-section, all Commonwealth of Virginia agencies shall report to VITA the following compliance information below no later than **January 31, 2022** and every January 31, thereafter.

Please complete the following:

1. Provide a certification statement that all employees and contractors have completed all required training.

   Click or tap here to enter text.

2. Provide a reason or justification that all employees/contractors have not completed all training.

   Click or tap here to enter text.

3. Provide an evaluation of the efficacy of the cybersecurity-training program that the agency provided

   Click or tap here to enter text.

4. Provide any suggestions on how VITA can improve the mandatory curriculum, materials, or any other aspects of the training program.

   Click or tap here to enter text.

ISO/AITR APPROVERS LIST

Please make sure your approver's list is updated and current. If there are personnel changes in your agency, work with your CAM to make sure the changes are reflective on your list.

You may request a copy of your agency's ISO/AITR list from the VCCC@vita.virginia.gov or tina.gaines@vita.virgina.gov

IS COUNCIL COMMITTEE SEEKING VOLUNTEERS FOR COMMITTEES

The next scheduled meeting for the IS Council:

March 16, 2022

Noon – 1 p.m. via Google Meets

If you would like an invite to the meeting, contact:

tina.gaines@vita.virginia.gov

SCANNING TARGETS

The web scanning team will be sending out emails requesting agency ISO's to verify their scanning targets so they can update their current list for 2022.

If you have questions, please send an email to commowealthsecurity@vita.virginia.gov.

QUESTIONS

MARCH 2022 ISOAG

March 2, 2022 from 1 to 4 p.m.

Presenters:

Debra Smith, VITA

David Brown

Marcus Thornton, Governor's Office

Herb Sening, Keith Hilliard and Grayson Walters, SAIC

VIRGINIA IT AGENCY

THANK YOU FOR ATTENDING!