Welcome and Opening Remarks

Mike Watson

March 4, 2020
• Welcome and Opening Remarks - Mike Watson

• NIST Publications 800-37 Risk Management- Eduardo Takamura, NIST Framework For Systems and Organizations

• How to Improve Cybersecurity – Servio F Medina, Health Information Technology

• Quantitative Risk Analysis – Mark Martens, VITA
NIST Risk Management Framework (RMF) Overview

Eduardo Takamura

FISMA Implementation Project
National Institute of Standards and Technology (NIST)
Information Technology Laboratory (ITL)
Computer Security Division (CSD)

Virginia Information Technologies Agency (VITA) Information Security Officer Advisory Group (ISOAG)
March 4, 2020 Meeting, Chester, VA
Outline

- Introduction
- NIST RMF Overview
- NIST RMF Steps
- Featured Publications
- Resources and Engagement Opportunities
- Q&A and Open Discussion

DISCLAIMER: any mention of entities, equipment, materials, or services throughout this talk is for information only; it does not imply recommendation or endorsement by NIST, nor is it intended to imply best available solution for any given purpose.
The National Institute of Standards and Technology (NIST) is a non-regulatory bureau of the U.S. Department of Commerce responsible for developing information security standards and guidelines, including minimum requirements for federal systems (except national security systems unless otherwise approved by appropriate federal officials exercising policy authority over such systems).


The Risk Management Framework (RMF) developed by NIST effectively brings together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.
The NIST Risk Management Framework

A flexible model for developing, implementing, and maintaining a risk management process for IT security and privacy


Provides a holistic risk management process (disciplined and structured)

Integrates information security and risk management activities into the system development life cycle

“to guide and inform the CATEGORIZATION of Federal information and information systems; the SELECTION, IMPLEMENTATION, and ASSESSMENT of security and privacy controls; the AUTHORIZATION of information systems and common controls; and the continuous MONITORING of information systems.” (Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource)
# NIST Special Publication 800-37 Revision 2

<table>
<thead>
<tr>
<th>HIGHLIGHTS</th>
<th>NEW GUIDANCE</th>
<th>UPDATED GUIDANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide closer links and <strong>improve communication</strong> between C-Suite/Governance-level to system/operational-level</td>
<td>Privacy, supply chain, Cybersecurity Framework (CSF), security engineering</td>
<td>Authorization boundaries</td>
</tr>
<tr>
<td>Integrates <strong>privacy, supply chain, and security engineering</strong> into the Risk Management Framework (RMF)</td>
<td>New Prepare Step</td>
<td>Authorization decisions and types</td>
</tr>
<tr>
<td>Aligns the <strong>Cybersecurity Framework</strong> and the RMF</td>
<td>All RMF tasks include potential inputs and expected outputs</td>
<td>Ongoing authorization</td>
</tr>
<tr>
<td>Demonstrates how the RMF is implemented in the <strong>system development life cycle</strong></td>
<td>“New” tasks in existing steps</td>
<td>Roles and responsibilities</td>
</tr>
</tbody>
</table>
NIST RMF Steps

INTRODUCTION OVERVIEW RMF STEPS PUBLICATIONS RESOURCES Q&A

PREPARE Step
CATEGORIZE Step
SELECT Step
IMPLEMENT Step
ASSESS Step
AUTHORIZE Step
MONITOR Step
**Prepare Step**

**Purpose:** Carry out essential activities at all three risk management levels to help prepare the organization to manage its security and privacy risks using the RMF.

### Organization- & Mission/Business Process-Level Tasks
- **P-1:** Risk Management Roles
- **P-2:** Risk Management Strategy
- **P-3:** Risk Assessment – Organization
- **P-4:** Organizationally-tailored Control Baselines and Cybersecurity Framework Profiles (optional)
- **P-5:** Common Control Identification
- **P-6:** Impact Level Prioritization (optional)
- **P-7:** Continuous Monitoring Strategy – Organization
- **P-8:** Mission or Business Focus

### System-Level Tasks
- **P-9:** System Stakeholders
- **P-10:** Asset Identification
- **P-11:** Authorization Boundary
- **P-12:** Information Types
- **P-13:** Information Life Cycle
- **P-14:** Risk Assessment – System
- **P-15:** Requirements Definition
- **P-16:** Enterprise Architecture
- **P-17:** Requirements Allocation
- **P-18:** System Registration

---

See Kelley Dempsey’s ISOAG June 7, 2017 presentation on ISCM
**Task Structure**

**INTRODUCTION**

**OVERVIEW**

**RMF STEPS**

**PUBLICATIONS**

**RESOURCES**

**Q&A**

---

**AUTHORIZATION BOUNDARY**

**TASK P-11** Determine the authorization boundary of the system.

- **Potential Inputs:** System design documentation; network diagrams; system stakeholder information; asset information; network and/or enterprise architecture diagrams; organizational structure (charts, information).

- **Expected Outputs:** Documented authorization boundary.

- **Primary Responsibility:** Authorizing Official.

- **Supporting Roles:** Chief Information Officer; System Owner; Mission or Business Owner; Senior Agency Information Security Officer; Senior Agency Official for Privacy; Enterprise Architect.

- **System Development Life Cycle Phase:** New – Initiation (concept/requirements definition). Existing – Operations/Maintenance.

- **Discussion:** Authorization boundaries establish the scope of protection for information systems (i.e., what the organization agrees to protect under its management control or within the scope of its...

- **References:** [SP 800-18]; [SP 800-39] (System Level); [SP 800-47]; [SP 800-64]; [SP 800-160 v1] (System Requirements Definition Process); [NIST CSF] (Core [Identify Function]).
## Prepare Tasks and Outcomes: Organization Level

<table>
<thead>
<tr>
<th>TASKS</th>
<th>OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TASK P-1: RISK MANAGEMENT ROLES</strong></td>
<td>Individuals are identified and assigned key roles for executing the RMF.</td>
</tr>
<tr>
<td><strong>TASK P-2: RISK MANAGEMENT STRATEGY</strong></td>
<td>A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.</td>
</tr>
<tr>
<td><strong>TASK P-3: RISK ASSESSMENT – ORGANIZATION</strong></td>
<td>An organization-wide risk assessment is completed or an existing risk assessment is updated.</td>
</tr>
<tr>
<td><strong>TASK P-4: ORGANIZATIONALLY-TAILORED CONTROL BASELINES AND CSF PROFILES (OPT)</strong></td>
<td>Organizationally-tailored control baselines and/or CSF profiles are established and made available.</td>
</tr>
<tr>
<td><strong>TASK P-5: COMMON CONTROL IDENTIFICATION</strong></td>
<td>Common controls that are available for inheritance by organizational systems are identified, documented, and published.</td>
</tr>
<tr>
<td><strong>TASK P-6: IMPACT-LEVEL PRIORITIZATION (OPT)</strong></td>
<td>A prioritization of organizational systems with the same impact level is conducted.</td>
</tr>
<tr>
<td><strong>TASK P-7: CONTINUOUS MONITORING STRATEGY – ORGANIZATION</strong></td>
<td>An organization-wide strategy for monitoring control effectiveness is developed and implemented.</td>
</tr>
</tbody>
</table>
## Prepare Tasks and Outcomes: System Level

<table>
<thead>
<tr>
<th>TASKS</th>
<th>OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TASK P-8:</strong> MISSION OR BUSINESS FOCUS</td>
<td>Missions, business functions, and mission/business processes that the system is intended to support are identified.</td>
</tr>
<tr>
<td><strong>TASK P-9:</strong> SYSTEM STAKEHOLDERS</td>
<td>The stakeholders having an interest in the system are identified.</td>
</tr>
<tr>
<td><strong>TASK P-10:</strong> ASSET IDENTIFICATION</td>
<td>Stakeholder assets are identified and prioritized.</td>
</tr>
<tr>
<td><strong>TASK P-11:</strong> AUTHORIZATION BOUNDARY</td>
<td>The authorization boundary (i.e., system) is determined.</td>
</tr>
<tr>
<td><strong>TASK P-12:</strong> INFORMATION TYPES</td>
<td>The types of information processed, stored, and transmitted by the system are id’d.</td>
</tr>
<tr>
<td><strong>TASK P-13:</strong> INFORMATION LIFE CYCLE</td>
<td>All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system.</td>
</tr>
<tr>
<td><strong>TASK P-14:</strong> RISK ASSESSMENT – SYSTEM</td>
<td>A system-level risk assessment is completed or an existing risk assessment is updated.</td>
</tr>
<tr>
<td><strong>TASK P-15:</strong> REQUIREMENTS DEFINITION</td>
<td>Security and privacy requirements are defined and prioritized.</td>
</tr>
<tr>
<td><strong>TASK P-16:</strong> ENTERPRISE ARCHITECTURE</td>
<td>The placement of the system within the enterprise architecture is determined.</td>
</tr>
<tr>
<td><strong>TASK P-17:</strong> REQUIREMENTS ALLOCATION</td>
<td>Security and privacy requirements are allocated to the system and to the environment in which the system operates.</td>
</tr>
<tr>
<td><strong>TASK P-18:</strong> SYSTEM REGISTRATION</td>
<td>The sys. is registered for purposes of management, accountability, coord. &amp; oversight.</td>
</tr>
</tbody>
</table>
**Purpose:** Inform organizational risk management processes and tasks by determining the adverse impact of the loss of confidentiality, integrity, and availability of organizational systems and information to the organization.

**C-1:** System Description  
**C-2:** Security Categorization  
**C-3:** Security Categorization Review and Approval
## Categorize Tasks and Outcomes

### INTRODUCTION

The characteristics of the system are described and documented.

### TASK C-1: SYSTEM DESCRIPTION

- A security categorization of the system, including the information processed by the system represented by the organization-defined information types, is completed.
- Security categorization results are documented in the security, privacy, and SCRM plans.
- Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission/business processes.
- Security categorization results reflect the organization’s risk management strategy.

### TASK C-2: SECURITY CATEGORIZATION REVIEW AND APPROVAL

- The security categorization results are reviewed and the categorization decision is approved by senior leaders in the organization.

### Security Objectives

- **CONFIDENTIALITY**
- **INTEGRITY**
- **AVAILABILITY**

### Impact Level

- **Low**: loss has limited adverse impact
- **Moderate**: loss has serious adverse impact
- **High**: loss has catastrophic adverse impact

---

For Distribution to NIST Personnel and Contractors Only

---

NIST Cybersecurity Framework Overview

---
**Select Step**

**Purpose:** Select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, and the Nation.

S-1: Control Selection

S-2: Control Tailoring

S-3: Control Allocation

S-4: Documentation of Planned Control Implementations

S-5: Continuous Monitoring Strategy – System

S-6: Plan Review and Approval
## Select Tasks and Outcomes

### INTRODUCTION

#### OVERVIEW

- NIST RMF Overview
- Publications
- Resources
- Q&A

<table>
<thead>
<tr>
<th>TASKS</th>
<th>OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TASK S-1: CONTROL SELECTION</strong></td>
<td>Control baselines necessary to protect the system commensurate with risk are selected.</td>
</tr>
<tr>
<td><strong>TASK S-2: CONTROL TAILORING</strong></td>
<td>Controls are tailored producing tailored control baselines.</td>
</tr>
<tr>
<td><strong>TASK S-3: CONTROL ALLOCATION</strong></td>
<td>- Controls are designated as system-specific, hybrid, or common controls.</td>
</tr>
<tr>
<td></td>
<td>- Controls are allocated to the specific system elements (i.e., machine, physical, or human elements).</td>
</tr>
<tr>
<td><strong>TASK S-4: DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS</strong></td>
<td>Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.</td>
</tr>
<tr>
<td><strong>TASK S-5: CONTINUOUS MONITORING STRATEGY – SYSTEM</strong></td>
<td>A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed.</td>
</tr>
<tr>
<td><strong>TASK S-6: PLAN REVIEW AND APPROVAL</strong></td>
<td>Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.</td>
</tr>
</tbody>
</table>
# Select Step: SP 800-53 Control Families

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC – AC</td>
<td>Access Control</td>
<td>PE – PE</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>AT – AT</td>
<td>Awareness and Training</td>
<td>PL – PL</td>
<td>Planning</td>
</tr>
<tr>
<td>AU – AU</td>
<td>Audit and Accountability</td>
<td>PM – PM</td>
<td>Program Management</td>
</tr>
<tr>
<td>CA – CA</td>
<td>Assessment, Authorization, and Monitoring</td>
<td>PS – PS</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>CM – CM</td>
<td>Configuration Management</td>
<td>PT – PT</td>
<td>PII Processing and Transparency</td>
</tr>
<tr>
<td>CP – CP</td>
<td>Contingency Planning</td>
<td>RA – RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>IA – IA</td>
<td>Identification and Authentication</td>
<td>SA – SA</td>
<td>System and Services Acquisition</td>
</tr>
<tr>
<td>IR – IR</td>
<td>Incident Response</td>
<td>SC – SC</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>MA – MA</td>
<td>Maintenance</td>
<td>SI – SI</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>MP – MP</td>
<td>Media Protection</td>
<td>SR – SR</td>
<td>Supply Chain Risk Management</td>
</tr>
</tbody>
</table>

**INTRODUCTION**

**OVERVIEW**

**RMF STEPS**

**PUBLICATIONS**

**RESOURCES**

**Q&A**
### Implement Step

**Purpose:** Implement the controls as specified in security and privacy plans for the system and for the organization, and update the plans with the as-implemented details.

I-1: Control Implementation  
I-2: Update Control Implementation Information

<table>
<thead>
<tr>
<th>TASKS</th>
<th>OUTCOMES</th>
</tr>
</thead>
</table>
| **TASK I-1: CONTROL IMPLEMENTATION** | • Controls specified in the security and privacy plans are implemented.  
  • System security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. |
| **TASK I-2: UPDATE CONTROL IMPLEMENTATION INFORMATION** | • Changes to the planned implementation of controls are documented.  
  • The security and privacy plans are updated based on information obtained during the implementation of the controls. |
**Purpose:** Determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and organization.

**A-1:** Assessor Selection  
**A-2:** Assessment Plan  
**A-3:** Control Assessments  
**A-4:** Assessment Reports  
**A-5:** Remediation Actions  
**A-6:** Plan of Action and Milestones
## Assess Tasks and Outcomes

<table>
<thead>
<tr>
<th>TASKS</th>
<th>OUTCOMES</th>
</tr>
</thead>
</table>
| **TASK A-1: ASSESSOR SELECTION** | • An assessor or assessment team is selected to conduct the control assessments.  
• The appropriate level of independence is achieved for the assessor or assessment team selected. |
| **TASK A-2: ASSESSMENT PLAN** | • Documentation needed to conduct the assessments is provided to the assessor or assessment team.  
• Security and privacy assessment plans are developed and documented.  
• Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required. |
| **TASK A-3: CONTROL ASSESSMENTS** | • Control assessments are conducted in accordance with the security and privacy assessment plans.  
• Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered.  
• Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments. |
| **TASK A-4: ASSESS. REPORTS** | Security and privacy assessment reports that provide findings and recommendations are completed. |
| **TASK A-5: REMEDIATION ACTIONS** | • Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken.  
• Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions. |
| **TASK A-6: PLAN OF ACTIONS AND MILESTONES** | A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. |
Authorize Step

**Purpose:** Provide accountability by requiring a senior management official to determine if the security and privacy risk to organizational operations and assets, individuals, other organizations, or the Nation of operating a system or the use of common controls, is acceptable.

**R-1:** Authorization Package

**R-2:** Risk Analysis and Determination

**R-3:** Risk Response

**R-4:** Authorization Decision

**R-5:** Authorization Reporting

**Decisions:**

- ✔️ Authorization To Operate
- ✔️ Common Control Authorization
- ✔️ Authorization To Use
- ✔️ Denial of Authorization

*New*
# Authorize Tasks and Outcomes

<table>
<thead>
<tr>
<th>TASKS</th>
<th>OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TASK R-1: AUTHORIZATION PACKAGE</strong></td>
<td>An authorization package is developed for submission to the authorizing official.</td>
</tr>
<tr>
<td><strong>TASK R-2: RISK ANALYSIS AND DETERMINATION</strong></td>
<td>A risk determination by the authorizing official that reflects the risk management strategy including risk tolerance, is rendered.</td>
</tr>
<tr>
<td><strong>TASK R-3: RISK RESPONSE</strong></td>
<td>Risk responses for determined risks are provided.</td>
</tr>
<tr>
<td><strong>TASK R-4: AUTHORIZATION DECISION</strong></td>
<td>The authorization for the system or the common controls is approved or denied.</td>
</tr>
<tr>
<td><strong>TASK R-5: AUTHORIZATION REPORTING</strong></td>
<td>Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.</td>
</tr>
</tbody>
</table>
Purpose: Maintain an ongoing situational awareness about the security and privacy posture of the system and the organization in support of risk management decisions.

M-1: System and Environment Changes
M-2: Ongoing Assessments
M-3: Ongoing Risk Response
M-4: Authorization Package Updates
M-5: Security and Privacy Reporting
M-6: Ongoing Authorization
M-7: System Disposal
## Monitor Tasks and Outcomes

<table>
<thead>
<tr>
<th>TASKS</th>
<th>OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TASK M-1: SYSTEM AND ENVIRONMENT CHANGES</strong></td>
<td>The information system and environment of operation are monitored in accordance with the continuous monitoring strategy.</td>
</tr>
<tr>
<td><strong>TASK M-2: ONGOING ASSESSMENTS</strong></td>
<td>Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy.</td>
</tr>
<tr>
<td><strong>TASK M-3: ONGOING RISK RESPONSE</strong></td>
<td>The output of continuous monitoring activities is analyzed and responded to appropriately.</td>
</tr>
<tr>
<td><strong>TASK M-4: AUTHORIZATION PACKAGE UPDATES</strong></td>
<td>Risk management documents are updated based on continuous monitoring activities.</td>
</tr>
<tr>
<td><strong>TASK M-5: SECURITY AND PRIVACY REPORTING</strong></td>
<td>A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.</td>
</tr>
<tr>
<td><strong>TASK M-6: ONGOING AUTHORIZATION</strong></td>
<td>Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.</td>
</tr>
<tr>
<td><strong>TASK M-7: SYSTEM DISPOSAL</strong></td>
<td>A system disposal strategy is developed and implemented, as needed.</td>
</tr>
</tbody>
</table>
Final Thoughts

RMF steps, tasks and supporting guidance facilitate and provide flexibility in the risk management process.

Not a one-size-fits-all approach or a compliance checklist.

Each organization is unique (i.e., may have different risks, threats, vulnerabilities, risk tolerance, and other attributes).

RMF development a product of collaboration; NIST public comment process (2 public comment periods); public workshops with industry; ever evolving.

Know what you have & know the risks.

Risks cannot be eliminated, they need to be reduced and managed.

Tips for streamlining RMF implementation on page 25 of NIST SP 800-37 Revision 2.
## Featured Publications

<table>
<thead>
<tr>
<th>Publication</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 199</td>
<td>Standards for Security Categorization of Federal Information and Information Systems</td>
</tr>
<tr>
<td>FIPS 200</td>
<td>Minimum Security Requirements for Federal Information and Information Systems</td>
</tr>
<tr>
<td>SP 800-30</td>
<td>Guide for Conducting Risk Assessments</td>
</tr>
<tr>
<td>SP 800-34</td>
<td>Contingency Planning Guide for Federal Information Systems</td>
</tr>
<tr>
<td>SP 800-39</td>
<td>Managing Information Security Risk: Organization, Mission, and Information System View</td>
</tr>
<tr>
<td>SP 800-53</td>
<td>Security and Privacy Controls for Federal Information Systems and Organizations</td>
</tr>
<tr>
<td>SP 800-53A</td>
<td>Assessing Security and Privacy Controls in Federal IS and Organizations</td>
</tr>
<tr>
<td>SP 800-53B</td>
<td>Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations <em>(planned)</em></td>
</tr>
<tr>
<td>SP 800-60 Vol. 1</td>
<td>Guide for Mapping Types of Information and Information Systems to Security Categories</td>
</tr>
<tr>
<td>SP 800-60 Vol. 2</td>
<td>Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices</td>
</tr>
</tbody>
</table>
### Featured Publications

<table>
<thead>
<tr>
<th>Publication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP 800-137</td>
<td>Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations</td>
</tr>
<tr>
<td>SP 800-137A</td>
<td>Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment <em>(planned)</em></td>
</tr>
<tr>
<td>SP 800-160 Vol. 2</td>
<td>Developing Cyber Resilient Systems: A Systems Security Engineering Approach</td>
</tr>
<tr>
<td>SP 800-161</td>
<td>Supply Chain Risk Management Practices for Federal Information Systems and Organizations</td>
</tr>
<tr>
<td>IR 8011</td>
<td>Automation Support for Security Control Assessments</td>
</tr>
<tr>
<td></td>
<td>• Vol. 1: <em>Overview</em></td>
</tr>
<tr>
<td></td>
<td>• Vol. 2: <em>Hardware Asset Management</em></td>
</tr>
<tr>
<td></td>
<td>• Vol. 3: <em>Software Asset Management</em></td>
</tr>
<tr>
<td></td>
<td>• Vol. 4: <em>Software Vulnerability Management</em> (est. March 2020)</td>
</tr>
</tbody>
</table>
# Resources and Engagement Opportunities

<table>
<thead>
<tr>
<th>INTRODUCTION</th>
<th>OVERVIEW</th>
<th>RMF STEPS</th>
<th>PUBLICATIONS</th>
<th>RESOURCES</th>
<th>Q&amp;A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FISMA Implementation Project Website</strong></td>
<td>![LEARN QR Code]</td>
<td>![PARTICIPATE QR Code]</td>
<td>![CONTRIBUTE QR Code]</td>
<td>![RESOURCES QR Code]</td>
<td>![Q&amp;A QR Code]</td>
</tr>
<tr>
<td><a href="https://csrc.nist.gov/Projects/risk-management">https://csrc.nist.gov/Projects/risk-management</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:sec-cert@nist.gov">sec-cert@nist.gov</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://csrc.nist.gov/Projects/risk-management/mailing-list">https://csrc.nist.gov/Projects/risk-management/mailing-list</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://csrc.nist.gov">https://csrc.nist.gov</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Computer Security Resource Center (CSRC) email updates</strong></td>
<td>![LEARN QR Code]</td>
<td>![PARTICIPATE QR Code]</td>
<td>![CONTRIBUTE QR Code]</td>
<td>![RESOURCES QR Code]</td>
<td>![Q&amp;A QR Code]</td>
</tr>
<tr>
<td><a href="https://public.govdelivery.com/accounts/USNIST/subscriber/new?qsp=USNIST_3">https://public.govdelivery.com/accounts/USNIST/subscriber/new?qsp=USNIST_3</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NIST Privacy Engineering Program</strong></td>
<td>![LEARN QR Code]</td>
<td>![PARTICIPATE QR Code]</td>
<td>![CONTRIBUTE QR Code]</td>
<td>![RESOURCES QR Code]</td>
<td>![Q&amp;A QR Code]</td>
</tr>
<tr>
<td><a href="https://www.nist.gov/privacy-engineering">https://www.nist.gov/privacy-engineering</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Resources and Engagement Opportunities

**INTRODUCTION**

**OVERVIEW**

**RMF STEPS**

**PUBLICATIONS**

**RESOURCES**

**Q&A**

<table>
<thead>
<tr>
<th><strong>Resource</strong></th>
<th><strong>Details</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>RMF 2.0 webcast</td>
<td><a href="https://go.usa.gov/xENcs">https://go.usa.gov/xENcs</a></td>
</tr>
<tr>
<td>RMF Training (2-hour, on-demand CBT)</td>
<td><a href="https://csrc.nist.gov/Projects/risk-management/rmf-training">https://csrc.nist.gov/Projects/risk-management/rmf-training</a></td>
</tr>
<tr>
<td>FCSM Forum Quarterly Meeting (April 21 &amp; July 23, 2020, Gaithersburg, MD)</td>
<td><a href="https://csrc.nist.gov/Projects/Forum/events">webcast option</a></td>
</tr>
<tr>
<td>FCSM Forum 2-Day Conference (October 28-29, 2020, Gaithersburg, MD)</td>
<td><a href="https://csrc.nist.gov/Projects/Forum/events">https://csrc.nist.gov/Projects/Forum/events</a></td>
</tr>
<tr>
<td>Advancing Cybersecurity Risk Management Conference (May 27-28, 2020, Gaithersburg, MD)</td>
<td><a href="https://go.usa.gov/xdqmX">https://go.usa.gov/xdqmX</a></td>
</tr>
</tbody>
</table>
STAY IN TOUCH

CONTACT US

sec-cert@nist.gov
privacyeng@nist.gov

@NISTcyber

- requires executive agencies with the federal government to **implement the RMF** that is described in NIST Special Publication 800-37  
- requires agencies to **integrate privacy** into the RMF process  
- addresses **responsibilities** for protecting federal information resources and for managing personally identifiable information (PII)  
- requires agencies to: **plan** for security; ensure that appropriate officials are assigned security **responsibility**; periodically **review** the security controls in their systems; **authorize** system processing prior to operations and, periodically, thereafter
A measure of the extent to which an entity is threatened by a potential circumstance or event

A function of:
- Adverse impact that would occur
- Likelihood of occurrence

Four Risk Factors:
- Threat
- Vulnerability
- Impact
- Likelihood
Organizational Risk

INTRODUCTION  OVERVIEW  RMF STEPS  PUBLICATIONS  RESOURCES  Q&A

threat source

initiates

threat event

exploits

vulnerability

casing

adverse impact

Organizational risk

to operations (mission, business functions, image, reputation), assets, individuals, or other organizations

Producing
**Risk Management Definitions**

```
“Risk Management: the program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.” (from NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy)

“Risk Management addresses protecting [Commonwealth of Virginia] information and IT systems commensurate with sensitivity and risk, including system availability needs. Accordingly, Risk Management is a central component of an agency information security program and allows each agency to determine how these factors apply to its IT systems and data.” (from Commonwealth of Virginia Information Technology Resource Management - Information Security Policy)
```
Risk Management Process

FRAME:
- Assumptions
- Constraints
- Tolerance
- Priorities & Tradeoffs

ASSESS:
- Threat & Vulnerability Identification
- Risk Determination

Assess

Information and Communication Flows

Frame

Monitor

Respond

RESPOND:
- Response identification
- Evaluation of alternatives
- Response decision
- Response implementation

MONITOR:
- Monitoring strategy
- Monitoring

INTRODUCTION OVERVIEW RMF STEPS PUBLICATIONS RESOURCES Q&A
Organization-Wide Risk Management

Three Levels of Organization-Wide Risk Management

Level 1: Organization (Governance)

Level 2: Mission/Business Process (Information and Information Flows)

Level 3: System (Environment of Operation)

Strategic Focus (Broad-based risk perspective)
Risk management across levels
Communication and reporting

Tactical Focus (Granular risk perspective)
## RMF Purpose

To ensure that managing risk from systems is consistent with mission/business objectives and the overall risk strategy established by the senior leadership through the risk executive (function)

To ensure that security and privacy requirements, including necessary controls, are integrated into the organization’s enterprise architecture and system development life cycle processes

To achieve more secure information and systems through the implementation of appropriate risk response strategies

To establish **responsibility and accountability** for the security and privacy of organizational systems/information/environments of operation

To provide senior leaders the necessary information to take credible, risk-based decisions with regard to the security and privacy of systems supporting organizational missions and business functions
## Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorizing Official</td>
<td>Risk Executive (Function)</td>
</tr>
<tr>
<td>Authorizing Official Designated Representative</td>
<td>Security or Privacy Architect</td>
</tr>
<tr>
<td>Chief Acquisition Officer</td>
<td>Senior Accountable Official for Risk Management</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>Senior Agency Information Security Officer</td>
</tr>
<tr>
<td>Common Control Provider</td>
<td>Senior Agency Official for Privacy</td>
</tr>
<tr>
<td>Control Assessor</td>
<td>System Administrator</td>
</tr>
<tr>
<td>Enterprise Architect</td>
<td>System Owner</td>
</tr>
<tr>
<td>Head of Agency</td>
<td>System Security or Privacy Officer</td>
</tr>
<tr>
<td>Information Owner or Steward</td>
<td>System Security or Privacy Engineer</td>
</tr>
<tr>
<td>Mission or Business Owner</td>
<td>System User</td>
</tr>
</tbody>
</table>
## Authorization Types, Options & Decisions

<table>
<thead>
<tr>
<th>Authorization Type</th>
<th>Other Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Authorization</td>
<td>Type Authorization</td>
</tr>
<tr>
<td>Ongoing Authorization</td>
<td>Facility Authorization</td>
</tr>
<tr>
<td>Reauthorization</td>
<td>Traditional or Joint Authorization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authorization Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization To Operate (ATO)</td>
</tr>
<tr>
<td>Common Control Authorization</td>
</tr>
<tr>
<td>Authorization To Use</td>
</tr>
<tr>
<td>Denial of Authorization</td>
</tr>
</tbody>
</table>
# NIST Frameworks

<table>
<thead>
<tr>
<th>NIST Frameworks</th>
<th>NIST Frameworks</th>
<th>NIST Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INTRODUCTION</strong></td>
<td><strong>OVERVIEW</strong></td>
<td><strong>RMF STEPS</strong></td>
</tr>
<tr>
<td>RISK MANAGEMENT FRAMEWORK (RMF)</td>
<td>CYBERSECURITY FRAMEWORK (RMF)</td>
<td>PRIVACY FRAMEWORK</td>
</tr>
<tr>
<td>Originally developed for federal information systems</td>
<td>Originally developed for Industrial Control Systems (ICS)</td>
<td>Established to meet the need for a common language and practical tool to address privacy needs.</td>
</tr>
<tr>
<td>Required for federal systems (per OMB A-130); can be adopted by any organization</td>
<td>Required for federal systems (per EO 13800); can be adopted by any organization</td>
<td>Voluntary framework; can be adopted by any organization</td>
</tr>
<tr>
<td>Seven steps: • Prepare • Categorize • Select • Implement • Assess • Authorize • Monitor</td>
<td>Five concurrent and continuous functions: • Identify (ID) • Protect (PR) • Detect (DE) • Respond (RS) • Recover (RC)</td>
<td>Five functions for managing privacy risks arising from data processing: • Identify-P • Govern-P • Control-P • Communicate-P • Protect-P</td>
</tr>
<tr>
<td>SP 800-53 control catalog is integrated into the framework (SELECT step)</td>
<td>Categories equivalent to control families in SP 800-53</td>
<td>Mapping to SP 800-53 controls (and to other informative references)</td>
</tr>
<tr>
<td>Flexible (customizable)</td>
<td>Adaptive to provide a flexible and risk-based implementation that can be used with a broad array of risk management (RM) processes</td>
<td>Flexible, modeled after the CSF</td>
</tr>
</tbody>
</table>
## NIST Frameworks

<table>
<thead>
<tr>
<th>RISK MANAGEMENT FRAMEWORK (RMF)</th>
<th>CYBERSECURITY FRAMEWORK (RMF)</th>
<th>PRIVACY FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of tiers to describe an increasing degree of rigor and sophistication in RM practices</td>
<td>Use of tiers to describe current (privacy) risk management practices, the degree of integration of privacy risk into the organization's enterprise risk management portfolio, the organization's data processing ecosystem relationships, and the organization's workforce composition and training program.</td>
<td></td>
</tr>
<tr>
<td>In-depth methodology</td>
<td>High(er) level of abstraction (comp. to the RMF)</td>
<td>High(er) level of abstraction (comp. to the RMF)</td>
</tr>
<tr>
<td>Aligned with CSF</td>
<td>Provides a <strong>common taxonomy</strong> and mechanism for organizations to:</td>
<td>Provides a <strong>common language</strong> to communicate privacy requirements with entities within the data processing ecosystem (particularly important when the data processing ecosystem crosses national boundaries such as international data transfers).</td>
</tr>
<tr>
<td>• Inputs &amp; outputs reference CSF as applicable;</td>
<td>• Describe their current cybersecurity posture;</td>
<td></td>
</tr>
<tr>
<td>• Task outcome tables reference CSF sections, categories or subcategories as applicable;</td>
<td>• Describe their target state for cybersecurity;</td>
<td></td>
</tr>
<tr>
<td>• References for tasks indicate relevant CSF sections (if any)</td>
<td>• Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;</td>
<td></td>
</tr>
<tr>
<td>Addresses security, privacy and supply chain risks</td>
<td>• Assess progress toward the target state;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Communicate among internal and external stakeholders about cybersecurity risk.</td>
<td></td>
</tr>
</tbody>
</table>

*Version 2.0* released December 2018  
Version 1.1 released April 2018  
Version 1.0 released in January 2020
When Cybersecurity Impacts Healthcare: How to Get to Yes
March 4, 2020

Presented to The Virginia Information Technologies Agency
About me

• Worked cybersecurity: ~18 years
• Taught college math: ~10 years
• Federal employee since 2013
• Three kids since 2013

Photo credit: Robyn Vaughan
Disclaimer

Content and opinions shared in this presentation, both written and verbal, are my own and not necessarily that of the Defense Health Agency or the Department of Defense.
Impacts to Healthcare

- Legally correct? Yes.
- Impacts healthcare? Also yes.

- Better?
- Necessary?

Recall WannaCry and cancelled NHS heart surgeries


https://www.mirror.co.uk/news/uk-news/fury-london-traffic-wardens-ticket-13222918
Example: 15-Minute Timeout/Screenlock

- Ticket for violation?
  - Control vulnerability: exploitation *has potential*
  - DoDIG finding

- Impact to healthcare?
  - Locked out during treatment
  - “Creative” workarounds

- How we got to yes
  - Conferred with PMO leadership

Photo credit: Servio Medina
Why Does this Happen?

<table>
<thead>
<tr>
<th>Situation</th>
<th>COA</th>
<th>Tenure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have an ailment?</td>
<td>Call the doc</td>
<td>Hippocrates (c. 460 - 370 BCE), &quot;father of modern medicine&quot;</td>
</tr>
<tr>
<td>Got a legal concern?</td>
<td>Consult OGC</td>
<td>1190 to 1230: folks began to practice canon law as a lifelong profession in itself</td>
</tr>
<tr>
<td>Impacted by Cybersecurity?</td>
<td>Maybe we aren’t really impacted...</td>
<td>The Morris Worm in 1983</td>
</tr>
</tbody>
</table>

Not to mention

- **IT/Cyber**: “you can’t patch stupid”
- **Provider**: “we’re saving lives – that’s my job”
- **PEO**: “can't transform a user with 8 hours of training…in a classroom”
All events described herein actually happened, though on occasion I’ve taken certain, very small, liberties with details, chronology, etc.
## Examples

<table>
<thead>
<tr>
<th>Possibly okay</th>
<th>NOT OKAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>15-Minute screen timeout</td>
<td>Wiggle mouse with elbow</td>
</tr>
<tr>
<td>Removing files when departing</td>
<td>20G of .PST and 3 years of files</td>
</tr>
<tr>
<td>Transmitting files <em>to/from</em> .mil, .gov, .com</td>
<td><em>from/to</em> non-GFE, including PII/PHI</td>
</tr>
<tr>
<td>Transfer files to/from government equipment</td>
<td>With flash drive</td>
</tr>
<tr>
<td>Saving files to the local shared drive; to cloud</td>
<td>Including PHI/PII</td>
</tr>
<tr>
<td>Transcription services</td>
<td>On CTR laptop, at CTR home</td>
</tr>
<tr>
<td>Using free/public web services</td>
<td>For healthcare scheduling</td>
</tr>
<tr>
<td>Defibrillator pulled from use in MTF</td>
<td>Because it had built-in, unauthorized WI-FI</td>
</tr>
<tr>
<td>Access DoD data/EHR</td>
<td>With personal device</td>
</tr>
<tr>
<td>Use Amazon Echo or Google Home</td>
<td>On your work desk (NOT kidding)</td>
</tr>
<tr>
<td>Text and email PHI</td>
<td>With personal equipment/account</td>
</tr>
<tr>
<td>Lab Analyzer kept on loading dock</td>
<td>No ATO (no RMF/assessment of risk)</td>
</tr>
<tr>
<td>Student Intern cannot access network/EHR</td>
<td>Background investigation takes too long; no CAC</td>
</tr>
<tr>
<td>Cybersecurity training</td>
<td>Sometimes the question doesn’t even make sense</td>
</tr>
</tbody>
</table>
Impact to Yes

- Lab Analyzer kept on loading dock - did not have an ATO or any RMF effort
- Saving PII/PHI to the local shared drive; to cloud
- DoD (MIL/CIV) official removing .PST and shared drive files when departing or retiring
- Student Intern (and even visiting provider) cannot access network “because” background investigation takes too long, no CAC
How to Get to Yes…*After Impact*

- **See Something? Say Something!**
  - Let someone know before trying a workaround: CIO, CMIO, ISSM…a Functional or other leader’s attention

- Report functional impacts of operational and technical issues that prevent full implementation and compliance

- Establish/Promote processes to support
Do something before it happens

- Bake cybersecurity into healthcare
- Equate poor cyber behavior with poor clinical care
- Make the right choice an easier choice
- Bake healthcare into cybersecurity

<table>
<thead>
<tr>
<th>Do Something</th>
<th>How Do Something</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bake cybersecurity in</td>
<td>What do providers need a year from now?</td>
</tr>
<tr>
<td>Poor cyber = Poor care</td>
<td>Cybersecurity part of patient safety - even after treatment</td>
</tr>
<tr>
<td>Right = Informed choice</td>
<td>Knowledge Base: <a href="https://info.health.mil/dadio/infosec/Pages/KnowledgeBase.aspx">https://info.health.mil/dadio/infosec/Pages/KnowledgeBase.aspx</a></td>
</tr>
<tr>
<td>Bake healthcare in</td>
<td>Get providers involved in messaging</td>
</tr>
</tbody>
</table>
If someone plugs in their personal smartphone to charge, should their network privileges be suspended?

Should the violator be required to take the same annual, cyber awareness training – you know, the same training they already took?

Should you have to take the driver’s license test again if you are caught speeding?
What’s the Point of Training?

Risky Behavior

<table>
<thead>
<tr>
<th>Risky Driving</th>
<th>Curb Risky Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reckless</td>
<td>Quick/frequent ticket</td>
</tr>
<tr>
<td>Texting</td>
<td>Increase risk awareness</td>
</tr>
<tr>
<td>W/o Seatbelt</td>
<td>Click it or Ticket</td>
</tr>
<tr>
<td>Fatigued</td>
<td>Rumble strips</td>
</tr>
</tbody>
</table>

Photo credit: Servio Medina
A nudge is any noncoercive alteration in the context in which people make decisions

- placing fruit at eye level in school cafeterias: enhances its popularity by as much as 25%

- a fly etched into the wells of urinals, giving male patrons something to aim at: spillage was reduced by 80%

Are “nudges” enough? What about an active shooter event?
US Airways Flight 1549 crash landed in the Hudson

Only 4 of 150 passengers properly put on their life vest

Source: WSJ
Airline Safety Videos

What’s wrong with this picture?

Source: CNN
Airline Safety Videos

Airline Safety Videos

Airline Safety Videos

Research suggests people remember some shows instead of the instructions

• **FLUENT**: leaders and their staffs need to be “cyber fluent” so they can fully understand the cybersecurity implications of their decisions. *2018 DoD Cyber Strategy*

• **FIT**: ongoing promotional campaign directed at 9.5M beneficiaries. *Defense Health Agency, 2016-Present*

• **HYGIENE**: cybersecurity hygiene = personal hygiene in that it is the individual’s responsibility; it includes all online behaviors. *2017 Health Care Industry Cybersecurity Task Force Recommendation*
Questions?

Feel free to contact me:
• servio.f.medina.civ@mail.mil

Plus ça change
Plus c'est la même chose
~Rush, Circumstances
Possibly (NOT) okay

• 15-Minute screen timeout. **Got to Yes:** memo signed by AO/CIO granting exception for OR and other restricted areas: up to 4 hours after coordination with PMO.

• Transmitting PII/PHI *to/from*.mil, .gov, .com –*from/to* non GFE. **Got to Yes:** DoD SAFE.

• Transfer files to government equipment from flash. **Getting to Yes:** depends on device, requires AO approval.

• CTR transcription services with non-GFE computer at home. **Got to Yes:** enforced a business associate agreement that already stipulated GFE for use.

• Using free/public web services for healthcare scheduling. **Getting to Yes:** bring IT (enterprise) capability needs through Governance

• Defibrillator pulled from use in MTF bc built-in wi-fi. **Got to Yes:** coordinated with MEDLOG

• Access DoD data/EMR with personal device. **Got to Yes:** Citrix/AVHE

• Use Amazon Echo or Google Home…on desk…at work (NOT kidding). **Getting to No?** OPSEC/Privacy policy prohibits recording/sending official business on non-GFE. BUT, this capability is in Every. Smart. Phone, so...

• Text and email PHI with personal equipment/account. **Getting to Yes:** understand the requirement and what is not working –*from the healthcare providers’ perspective*

• Cybersecurity training answers and *even questions* do not make sense to some providers. **Getting to Yes:** provide contextually meaningful training supplemental to vice relying on the 1 hour of mandatory training.
Quantitative Cyber Risk Analysis

Risk Management Team
Commonwealth Security and Risk Management

3/4/2020
Objective

• To develop an accurate and defendable methodology to estimate costs associated with the detection, response, and recovery activities associated with cyber security incidents within the Commonwealth Executive Branch, independent agencies and institutions of higher education.
Purpose

- Provide Executive leadership an enhanced ability to make informed risk based decisions:
  - IT Investments
  - Security enhancements
  - Security exceptions
  - Cyber liability insurance
  - Protect AAA Bond Rating
  - Understand the reputational risks
Model Component Definitions

• Baseline risk
  – Risk incurred for agencies with basic cyber hygiene program
  – Each application measured for likelihood of breach and impact of breach

• Residual risk
  – Risk incurred by the Commonwealth after identifying missing security controls
  – Missing controls increase the likelihood of a breach

• Loss Event cost estimate
  – Based on industry trends and Commonwealth costs
  – Formula based on line of best fit for data collected
Data Breach Cost Calculation

- As the number of compromised records increases, the cost exponentially decays.

- Commonwealth analysis produced a cost factor of $4,812.60 for 2019.

- Industry estimates include direct and indirect response cost.

$$y = (4812.6)(x^{-0.358})$$
Data Breach Cost Range

• Industry standard is the high end of the range

• Data breaches result in both direct and indirect costs
  – Direct cost is direct expense outlay to resolve the breach
  – Indirect cost is time, effort and other organizational resources allocated to data breach resolution

• Commonwealth analysis removes some of the indirect costs associated with a data breach
Reputational Risk

- Represented by the number of citizens impacted by an incident

- May not directly correlate with the number of records impacted
  - Public safety
  - Transportation infrastructure
  - Critical infrastructure
APPLICATION RISK INFORMATION

- Default Records at Risk: 3,000
- Records at Risk Override:
- Application Baseline $273,886
- Application Residual $821,659
Application inherent risk

- This field utilizes either the default records at risk or the override as stated earlier, and uses the formula previously covered in order to determine the financial risk associated with the application.
Records at Risk Override

• If this field is filled out by the AITR, it will be used instead of the default.
Application Residual Risk

• This field takes the Inherent Risk Field and modifies it based upon the open findings, and their association to the CIS top 20 controls.
Application Residual Risk Calculation

• For each CIS control that the application doesn't meet, it will increase the risk, by 8% for Basic controls (1-6), 4% for foundational controls (7-16), and 3% for organizational controls (17-20), the maximum being 200%. However, if there is no audit or risk assessment completed, there is instead a 3x multiplier placed on it.
Help Text

• Can be found on the above fields, and should help somewhat in clarifying them.
Questions
Upcoming Events
COV Information Security Conference

2020 vision: A future of innovation

April 16 & 17

Richmond, VA
2020 Security Conference Registration and Call for Papers

Registration for the 2020 Commonwealth of Virginia (COV) Information Security Conference is now open. The conference will be held on April 16 & 17 at the Altria Theater in Richmond. Deadline for Call for Papers is March 6.

Conference Cost: $175

Conference and registration information can be found on the link below.

*For all other conference questions: covsecurityconference@vita.virginia.gov*
Keynote Speaker – Day One

Susie Adams, Chief Technology Officer
Microsoft Federal
Keynote Speaker – Day One

Larry Weaver
Professional Comedian and Business Leader
The next IS Orientation will be held on March 31, 2020
1p-3p in room 1211 (CESC)
Presenter: Marlon Cole (CSRM)

Registration Link:
http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10
Arlyn Burgess

**Data Science opportunities and barriers: The power of partnership**

UVA School of Data Science

Alan Gernhardt

**Public Records**

Virginia Freedom of Information Advisory Council

Eric Culbertson

**MSS Web Content Reporting Tool**

ATOS
THANK YOU FOR ATTENDING