FEDERAL COMPUTER SECURITY MANAGERS' (FCSM) FORUM: THE DEPARTMENT OF VETERANS AFFAIRS (VA)

Dominic Cussatt

Chief Information Security Officer

Office of Information Security (OIS)

May 15, 2018

VA | U.S. Department of Veterans Affairs
Office of Information and Technology

Agenda

This presentation comprises information relative to VA's cybersecurity program including VA's relationship with the Office of Inspector General (OIG), VA's transition to the Enterprise Cybersecurity Strategy Program (ECSP), and VA's alignment with Federal Guidelines.

1. Setting the Stage: VA by the Numbers
2. VA OIG Remediation Efforts
3. VA Enterprise Cybersecurity Strategy Team (ECST) Remediation Accomplishments
4. The Transition from ECST to Enterprise Cybersecurity Strategy Program (ECSP)
5. VA's Alignment with National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and Cybersecurity Framework (CSF)
6. Looking Forward: VA's Partnership with DoD

"To care for him who shall have borne the battle, and for his widow, and his orphan."

-President Abraham Lincoln

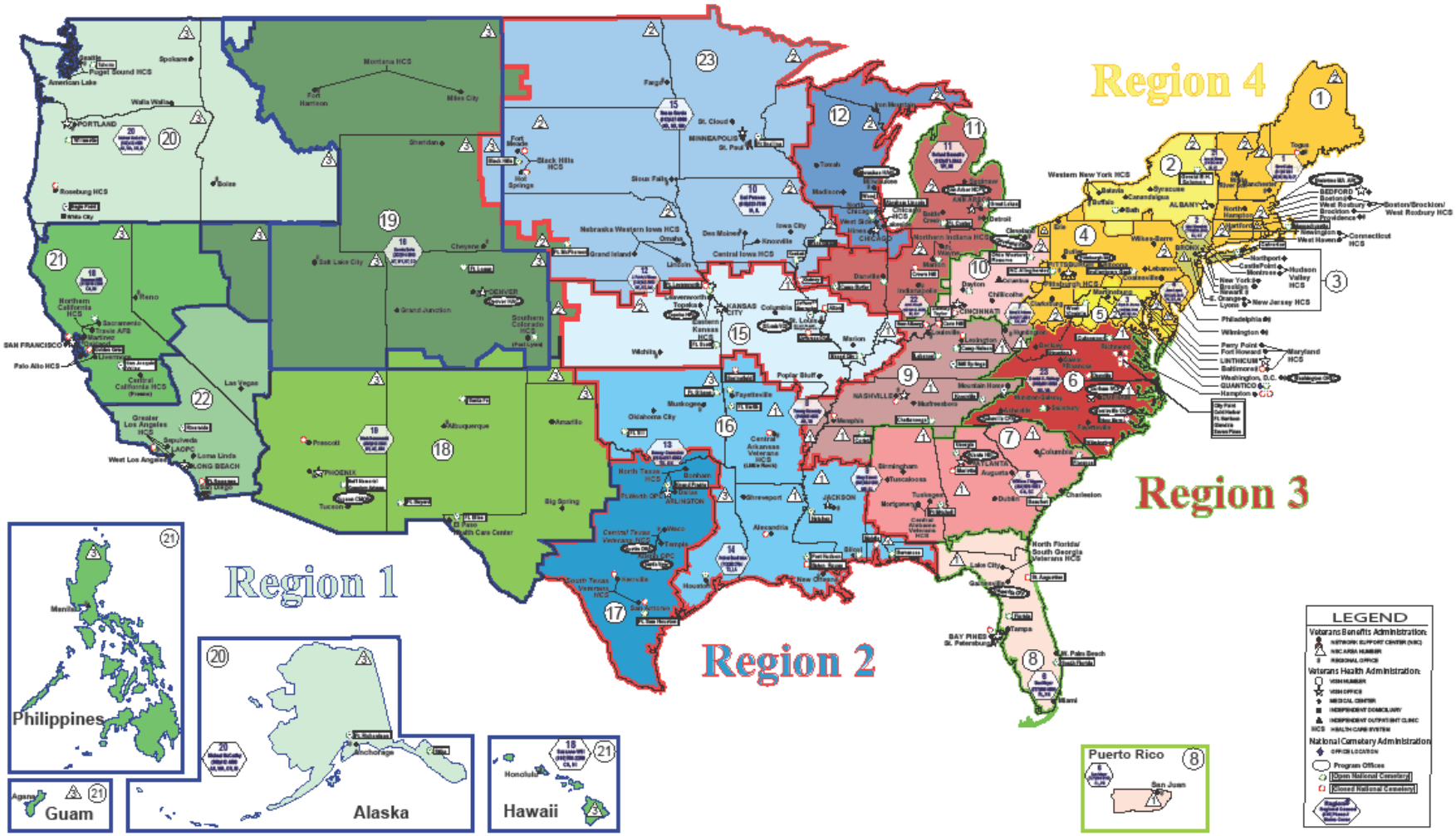
"I think both the President and I believe not only have veterans earned this, but this [fixing VA systems] is actually a matter of national security."

-Former VA Secretary Dr. David Shulkin

VA by the numbers...

- 3 Administrations and 3 Major Functions: Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), National Cemeteries Administration (NCA)
- Second Largest US Federal Agency
- VA Is the Size of a Fortune 10 Company
- $186B Annual Operating Budget
- $4B Annual IT Budget
- $400M Annual Cybersecurity Budget
- 350,000+ Federal Employees Across the US and Abroad
- VA Supports 20 Million US Veterans
- 145 Hospitals and 1,231 Outpatient Facilities, making VA the largest Health Care Organization in the US
- 56 Regional Benefits Offices
- 135 Veteran Cemeteries

Department of Veterans Affairs



VA Benefits & Health Care Utilization

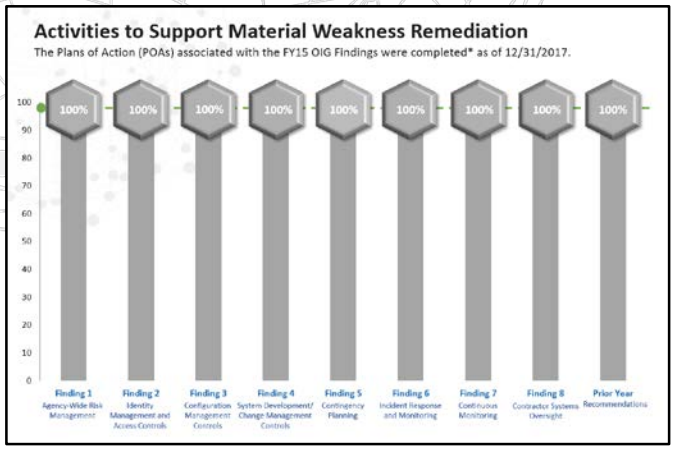
Updated 1/25/18

Number of Veterans Receiving VA Disability Compensation (as of 12/31/17):	4.60 M
Number of Veterans Rated 100% Disabled (as of 12/31/17):	625,947
Number of Veterans Receiving VA Pension (as of 12/31/17):	272,712
Number of Spouses Receiving DIC (as of 12/31/17):	396,823
Number of Total Enrollees in VA Health Care System (FY 17):	9.12 M [1]
Number of Total Unique Patients Treated (FY 17):	6.41 M [1]
Number of Veterans Compensated for PTSD (as of 12/31/17):	978,226
Number of Veterans in Receipt of IU Benefits (as of 12/31/17):	351,333
Number of VA Education Beneficiaries (FY 17):	946,829
Number of Life Insurance Policies Supervised and Administered by VA (as of 12/31/17):	6.06 M
Face Amount of Insurance Policies Supervised and Administered by VA (as of 12/31/17):	1.22 T
Number of Veterans Participating in Voc Rehab (Chapter 31) (FY 17):	132,218[3]
Number of Active VA Home Loan Participants (as of 12/31/17):	2.96 M
Number of Health Care Professionals Rotating Through VA (Academic Year (AC) 17):	122,949
Number of OEF/OIF Amputees (as of 1/01/18):	1,718[2]

Source: VBA Office of Performance Analysis and Integrity; Health Services Training Report; VBA Education Service; [1] VHA OABI and VSSC (10E2A); [2] DoD. Produced by the National Center for Veterans Analysis and Statistics; [3] Includes 1,651 Veterans in interrupted case status over one year.
http://www.va.gov/vetdata/pocketcard/index.asp

VA OIG Remediation Efforts

VA has been committed to remediating the OIG's findings and improving the agency's overall security posture. In response to the OIG FY15 FISMA report, VA developed and implemented plans associated with the 35 OIG FY15 FISMA Audit recommendations. The plans of action (POAs), took on a new approach to strategically tackle the findings going forward.



Under the ECST, POAs were designed to capitalize on efficiencies (e.g., use of existing tools and licenses) and to incorporate the previous findings along with the new findings from the FY15 FISMA audit.

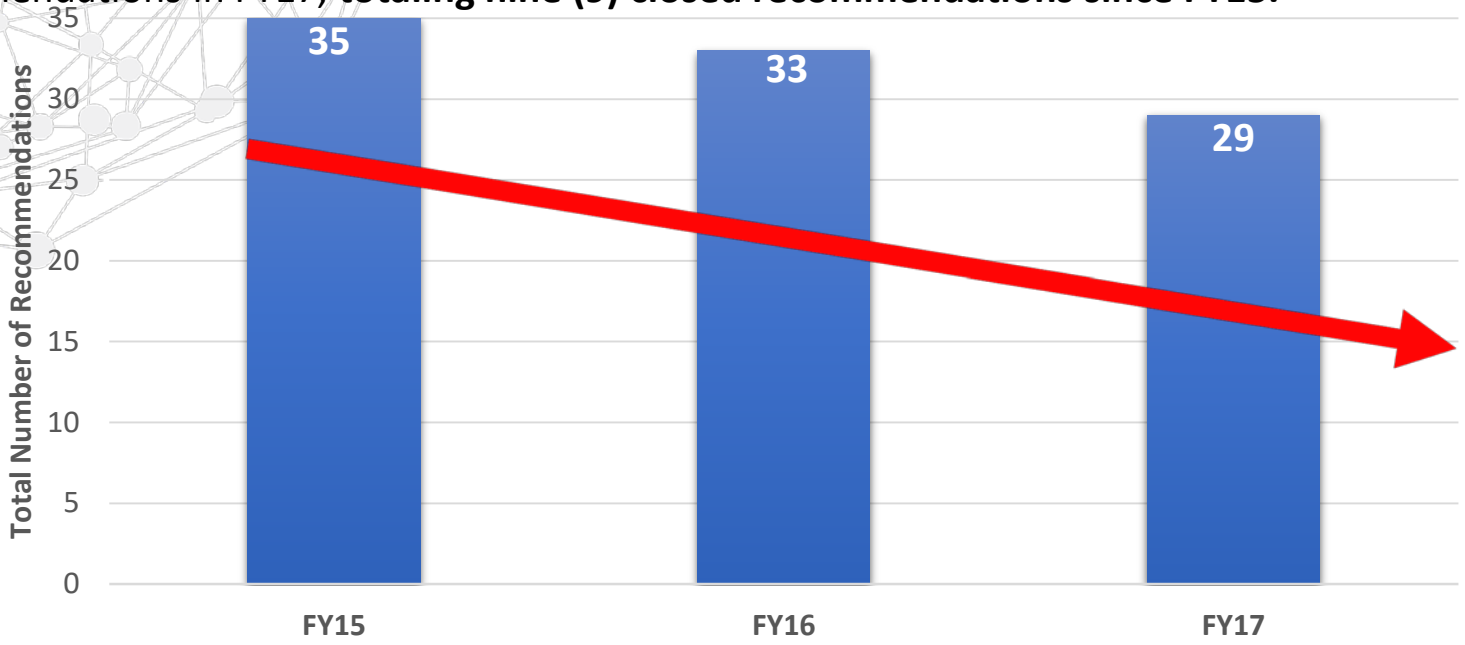
The POA effort was completed at the end of calendar year 2017.

We have made improvements in our security posture from FY15 to FY17. We continue to decrease the total number of recommendations for improving VA's information security program year after year. From FY15 to FY17, we have closed a total of nine (9) recommendations.

Sources: Enterprise Cybersecurity Strategy Team (ECST) Corrective Action Plan Update. 06/01/2017 / Audit Status Chief Financial Officer (CFO) Briefing. 01/23/2018 / Cybersecurity Policy Compliance Analytics Support (CSPCAS) 5.4.1 (D) Quarterly Executive Summary Report. 03/05/2018

VA OIG Remediation Efforts – Continued Progress

A review of the FY15-FY17 OIG FISMA Audit Reports indicates that VA has decreased the total number of recommendations for improving VA's information security program. From FY15 to FY16, OIG reported that **VA closed five (5) OIG recommendations**; however, OIG also identified three (3) new recommendations in FY16. Moreover, VA successfully closed an additional four (4) recommendations in FY17, **totaling nine (9) closed recommendations since FY15.***



New / Closed Recommendations	2016	2017	Total
# New Recommendations	3 ↑	0 ↔	3 ↑
# Closed Recommendations	5 ↓	4 ↓	9 ↓

Net decrease of 6 recommendations from FY15 to FY17

*Information herein was developed from the final FY15 and FY16 OIG FISMA Audit Reports, as well as the draft FY17 OIG FISMA Audit Report. **In response to the Material Weakness identified during the FY15 OIG FISMA audit, VA created individual Plans of Action (POAs) to address tactical security issues and were not established prior to the FY15 OIG FISMA audit.

VA ECST Remediation Accomplishments

Below are some accomplishments associated with the completion of the POAs, which were based on the FY15 OIG findings. These accomplishments stem from the 35 ECST POAs that were created and completed in response to the FY15 OIG FISMA audit.

Contingency Planning:
Developed Standard Operating Procedures (SOPs) to apply standards and practices developed within VA **to define backup tape retention policies, a data loss migration strategy, disaster recovery, and data protection standards for agency-wide backup strategy**

Identity Management and Access Controls:
Reduced the number of elevated privileged user accounts for employees and contractors by **96%** since mid-2015

Configuration Management Controls:
Implemented the DbProtect database scanning tool, **which enables VA to perform blocking, locking, and termination functions when malicious activity is detected**; and integrated it with the Nessus Enterprise Web Tool (NEWT), **which provides an automated analysis of our multiple security scans**

Agency – Wide Risk Management Program: Updated the Assessment and Authorization (A&A) process by **focusing on increasing System Owner accountability in order to reduce the number of systems with an expired Authority to Operate (ATO)**

Change Management Controls:
Developed and provided **training and accountability for VA personnel** with change management responsibilities

Contractor Systems Oversight:
Revised and created policies **in order to address cloud security policy gaps**

Incident Response and Monitoring:
Published VA Directive and Handbook 6513: Secure External Connections, **governing the process for managing and continuously monitoring VA connections**

Sources: Progress reported by VA lead and reflects accomplishments reported as of 03/30/2018 / CRISP Remediation Services Support (RSS) Update 03/30/2018

Enterprise Cybersecurity Program Overview

VA evaluated their 2015 Enterprise Cybersecurity Strategy as well as the ECST program. VA then took a step back to analyze where they have had successes, and where they needed to shift their priorities. VA then evolved their program from the ECST to the ECSP, where they plan to continually evaluate, prioritize, and evolve so they can stay ahead of the dynamic and ever-changing threat landscape, Federal statutes and requirements, and feedback from their partners and OIG.

ECST

July 2015:
In response to the Office of Management and Budget (OMB) M-16-04 "Cybersecurity Implementation Plan (CSIP)", VA formed the ECST, to tackle VA's longstanding challenges to enterprise cyber resiliency. The ECST has focused on the following:

Strategy:
Eight (8) Domains created as a result of VA's 2015 Enterprise Cybersecurity Strategy

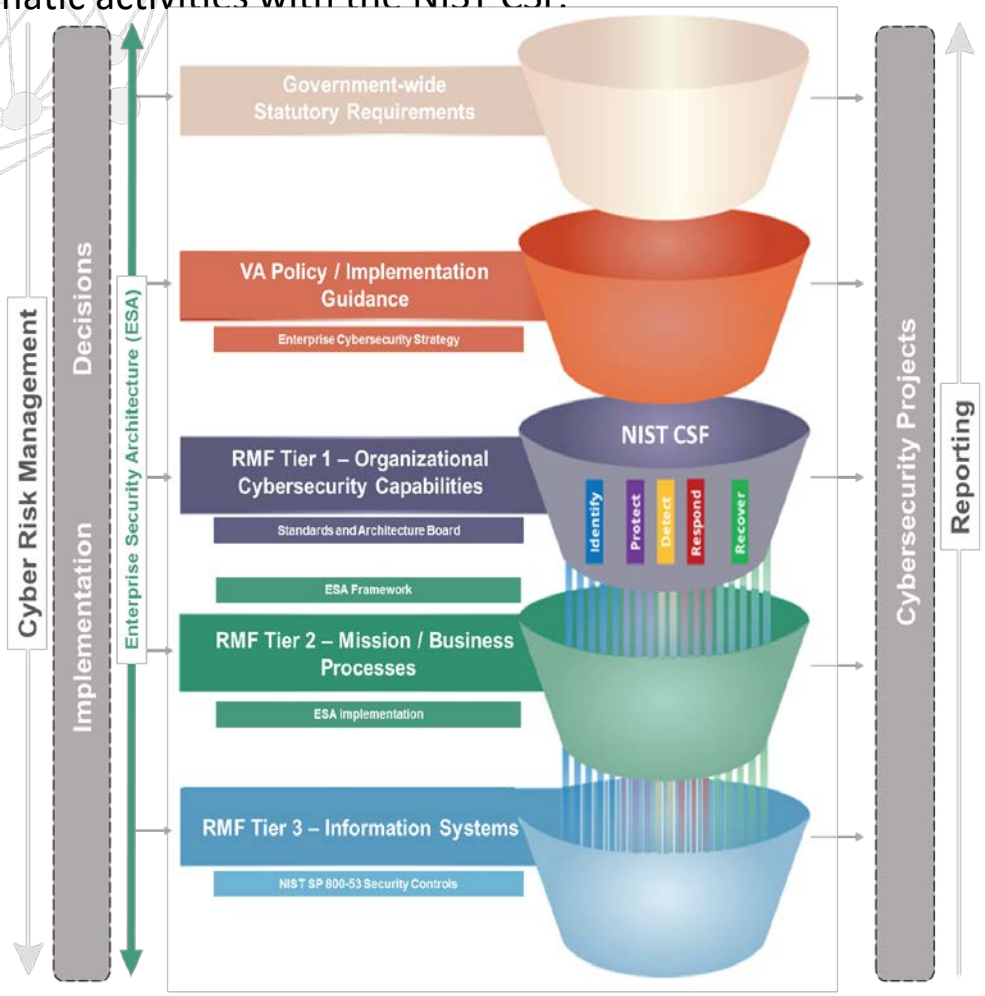
Remediation:
35 POAs created in response to the FY15 OIG FISMA audit

ECSP

- Create a program that spans from government-wide statutory requirements to the information system level
- Align VA with the NIST CSF
- Enable prioritization of cybersecurity projects

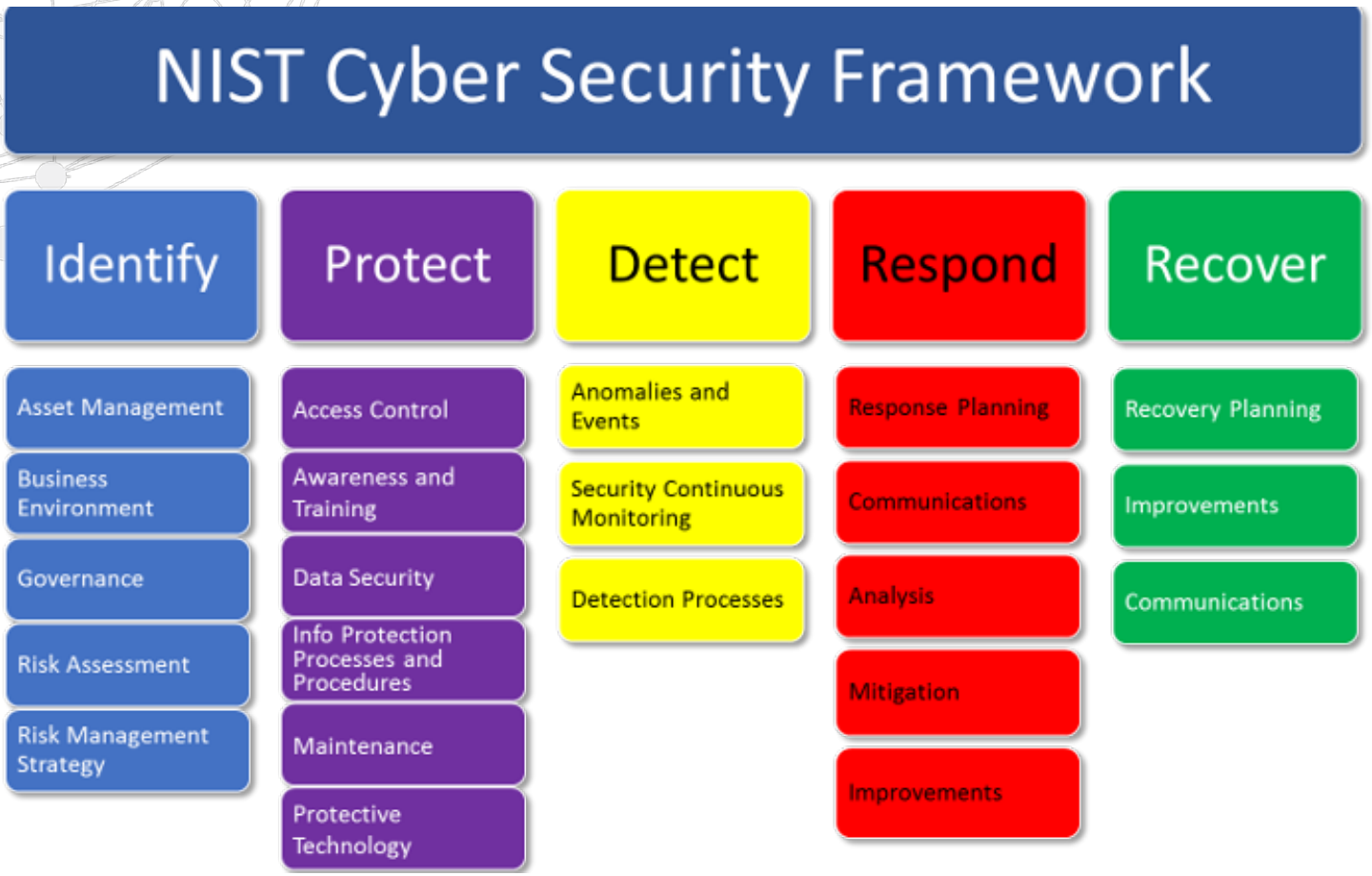
NIST CSF and the ECSP

In response to Presidential Executive Order (EO) 13800 on “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”, each federal agency is required to use the NIST CSF to manage the agency's cybersecurity risk. Through the ECSP, VA aims to make prioritized, defensible decisions related to the implementation of cybersecurity projects (that may be technical or procedure-based), and align programmatic activities with the NIST CSF.



NIST CSF and the ECSP (Continued)

The CSF provides agency-level visibility into cybersecurity capabilities and outcomes, while the RMF generates system-level risk indicators that, when rolled up to the agency-level focus of the CSF, create a comprehensive risk management program under the ECSP. The VA Cyber Security Operations Center (CSOC's) core functions map directly to the NIST CSF.



NIST RMF and the ECSP

When VA implemented the NIST CSF, they wanted to rely upon as much of the existing RMF program as they could, so they've incorporated data from their RMF process to inform the prioritization of activities under the auspices of the NIST CSF. To that end, VA was very well positioned ahead of the release of the May 2017 EO on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, and so had a head start on implementing an agency-wide approach that standardizes the organizational management of identified risks.

Risk Scoring

ID	NIST Control Title	VA Common Control	Cited in NFR	Impacted by HIPAA	Included in "CIS Top 20" Report	Confidentiality	Integrity	Availability	Risk Score	Risk Level
CA-02.1	Security Assessments	No	FY16 & FY17	Yes	Yes	Yes	Yes	Yes	857	High

The risk criteria for CA-02.1 results in a risk score of 857, a high risk control

The Prioritization Tool

Project Information					
Project Rank Order	Project No. / Identifier	Project Name	Project Description	Tangible Outcomes	Source
11	0015	Implement Enterprise Mission Assurance Support Service (eMASS)	VA's GRC refresh initiatives and eMASS implementation through Fiscal Year (FY) 2018 will provide automation to support ongoing security documentation updates that will reflect the current operating environment. In addition, These initiatives enable better visibility and increased identification of risk across the information system landscape. Additionally, they will improve uniformity and accountability so that VA leadership has better insight into information system risks affecting VA's	Updated GRC tool (eMASS) implemented	Other | FY17 OIG FISMA Audit Report

Prioritization Factors						
Priority Score	OIG's Notice of Finding & Recommendation (NFR)	Risk Score	External Factors	Internal Factors	Time Sensitivity	Strategic Alignment
578.11	Yes	857	None	VA C-Suite Leadership Objectives / Priorities	None	Yes

As the highest risk control associated to the project, the risk score for CA-02.1 is used as a prioritization factor

Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37

NIST RMF and the ECSP (Continued)

The RMF provides VA with the ability to assess compliance, measure operational risk, and ultimately make risk-based determinations for an information system's Authority To Operate (ATO). VA RMF is the foundation where system-level risk is aggregated and driven up to the CSF to allow VA executives to make risk-based decisions from both a systems and agency perspective in alignment with cybersecurity capabilities.

Step 1
CATEGORIZE
System

- Categorize the system based on potential loss of confidentiality, integrity, or availability
- Initiate Security Plan
- Assign qualified personnel to RMF roles

Step 2
SELECT
Security Controls

- Select security controls
- Tailor initial security control set
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy

Step 3
IMPLEMENT
Security Controls

- Implement control solutions
- Document security control implementation in Security Plan

Step 4
ASSESS
Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5
AUTHORIZE
System

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

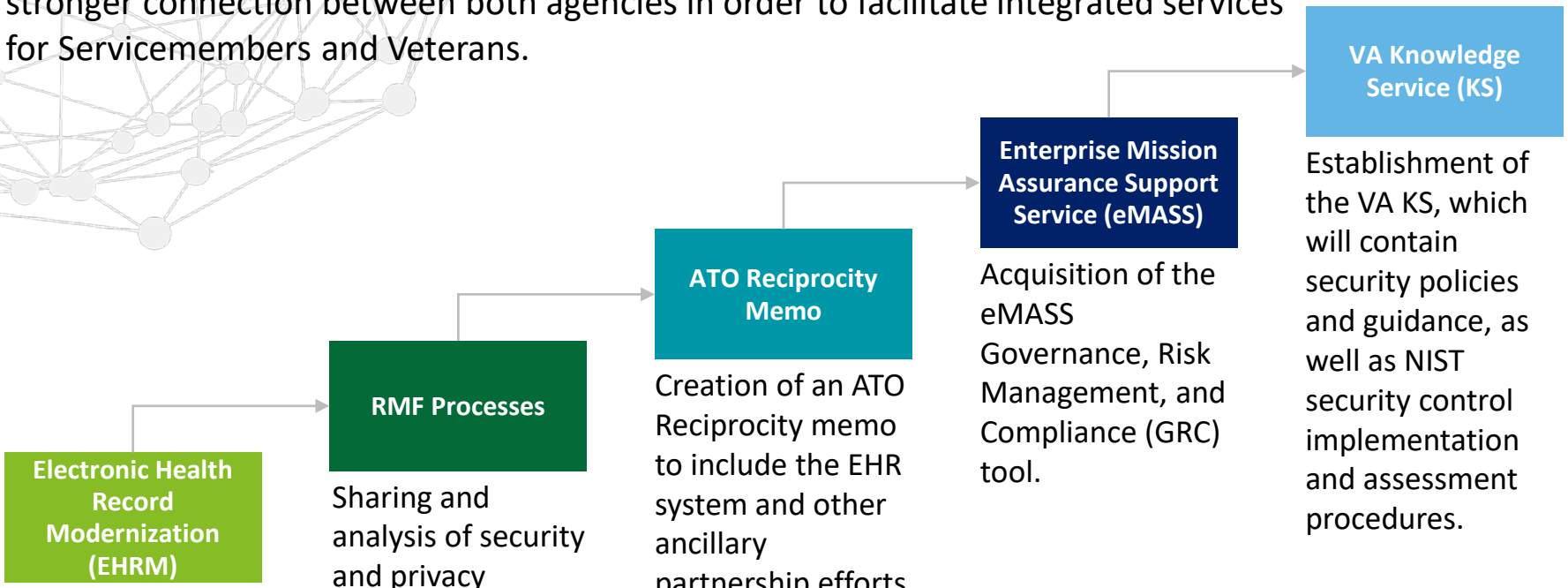
Step 6
MONITOR
Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37

Looking Forward: Our Partnership with DoD

As part of VA's mission to serve and honor Veterans, VA is collaborating with the DoD across multiple information technology domains, specifically information security. The goal of this collaboration is to provide uninterrupted service to the armed forces during the transition from active duty to Veteran status. VA seeks to further build on the momentum with DoD and create a stronger connection between both agencies in order to facilitate integrated services for Servicemembers and Veterans.



Source: VA Secretary Announces Decision on Next-Generation Electronic Health Record, 6/5/2017