CSIP, CNAP, FY16 FISMA & Beyond

NIST CSF V1.0

Disclaimer

- Not an expert
- Not representing Deloitte
- Deloitte slide decks are infinitely more polished

ISSA-NOVA SIG RMF Lifeboat

- Collaborative Network Defense
- Field Guide to Using RMF, Steps 1-3
- Assessing Large Multi-Agency Network Defense
- How to Reduce Impact of a Cyber Black Swan Event
- CyberSprint & FY16 FISMA
- Cloud Risk Mgmt & DevOps Pipeline
- Digital Forensics in the Cloud
- Enhanced Situational Awareness in the Cyber Landscape

**** Find us on Meetup or ISSA-NOVA websites. See Resources links.**

Agenda

- CyberSprint
- Cybersecurity Strategy & Implementation Plan (CSIP)
- NIST Cybersecurity Framework (CSF)
- Cybersecurity Metrics
- Cybersecurity National Action Plan (CNAP)

Source: One-time use license from The Cartoonist Group: cartoonistgroup.com

Cyber Sprint

- May- June 2015 – Response to OPM breach
- 30-day ‘marathon’ review of Gov’t cyber policies, procedures, and practices.
- High value assets
- Patching critical vulnerabilities
- Privileged users
- Multi-factor authentication adoption
- Operationalize action plans and strategies for critical cybersecurity priorities
- Recommend a Federal Civilian Cybersecurity Strategy

OMB Memoranda for Heads of Executive Departments and Agencies

Number	Subject	Author	Date
M-16-03	Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements	Shaun Donovan (Director)	October 30, 2015
M-16-04	Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government	Shaun Donovan (Director) & Tony Scott (Federal Chief Information Officer)	October 30, 2015
Version 1.0 Version 1.1	FY 2016 CIO FISMA Metrics FY 2016 IG FISMA Reporting Metrics	DHS/OMB DHS/OMB	October 1, 2015 July 29, 2016

The Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Gov't (M-16-04)

- CSIP directs a series of actions to improve capabilities to identify and detect vulnerabilities and threats, strengthen protections of government assets/information, and develop enhanced response/recovery capabilities to allow readiness/resilience when incidents occur
- Broader series of actions to improve Federal civilian cybersecurity, including:
  - ✓ Updated FISMA guidance
  - ✓ Revisions to *Circular A-130, Managing Info as a Strategic Resource*
  - ✓ New guidance on implementing cybersecurity contracting language
  - ✓ Cyber incident response best practices
  - ✓ BPA for Identity Protection Services to give Federal agencies access to best-in-class solutions
  - ✓ Updated Cybersecurity Cross-Agency Priority (CAP) Goal

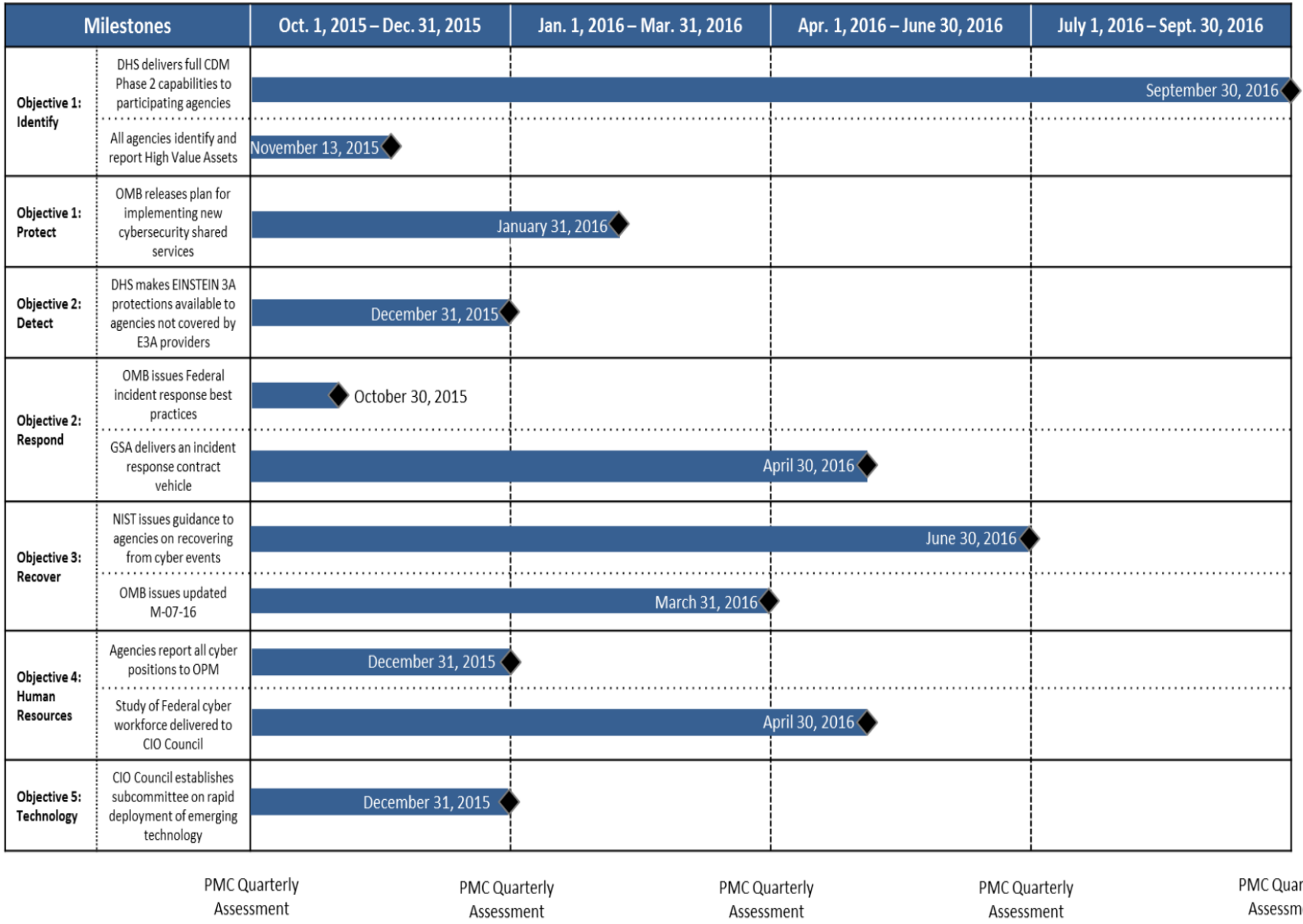
CSIP Key Actions

1. Agencies will continue to identify their **high value assets** (HVAs) and critical systems to understand their potential impact from a cyber incident, and ensure robust physical and cybersecurity protections are in place.
2. DHS will accelerate the deployment of **Continuous Diagnostics and Mitigation (CDM) and EINSTEIN** capabilities to all participating Federal agencies to enhance detection of cyber vulnerabilities and protection from cyber threats. DHS is extending E3's capabilities for behavioral analytics.
3. All agencies will improve the **identity and access management** of user accounts on Federal information systems to drastically reduce vulnerabilities and successful intrusions.
4. OMB, in coordination with NSC and DHS, will issue **incident response** best practices for use by Federal agencies. *CSIP directs agencies to patch all vulnerabilities immediately or, at min,* ***within 60 days of patch release.***

CSIP Key Actions

5. NIST will provide improved guidance on how to recover from cyber events.
6. OPM and OMB will initiate several new efforts to improve Federal cybersecurity **workforce recruitment, hiring, and training** and ensure a pipeline for future talent is put in place. ***(Lots of interesting ideas.)***
7. The CIO Council will create an Emerging Technology Sub-Committee to facilitate efforts to **rapidly deploy emerging technologies** at Federal agencies. (DARPA, HSARPA, NSF, NCCoE, etc.) ***GSA developing procurement vehicles to allow agencies to access technology at any Fed tech incubator.***
8. CIOs and CISOs will have direct **responsibility and accountability for CSIP implementation**, consistent with their role of ensuring the identification and protection of their agency's critical systems and information.

CSIP Milestones



FY 2015-2016 Guidance on Federal Information Security and Privacy Mgmt Requirements (M-16-03)

Section I: Information Security and Privacy Program Oversight and Reporting Requirements

- ✓ Timelines and requirements for quarterly & annual reporting
- ✓ Directions for preparing annual agency FISMA reports to be submitted to DHS through CyberScope
- ✓ Defines a "Major Incident" (per Congressional requirement)

Section II: Incident Response Coordination Activities

- ✓ Best practices based on lessons learned from the major FY15 cybersecurity incidents and CyberSprint assessments
- ✓ At minimum, agency CIO and CISOs need TS SCI access for classified malicious-actor TTPs.
- ✓ Provides mechanism by which agencies can ask/receive on-site, technical assistance from DHS during incident response

'Major Incident' Notification

- Victim agency is responsible for determining whether the incident is considered "major."
- DHS is required to notify OMB within one (1) hour of the relevant agency notifying DHS of the "major" incident.
- Agencies are to notify Congress within 7 days of the date when the incident was determined to be "major."
- Congress requires agencies to follow-up with additional information regarding threats, actors, risks, status of affected system, detection, response, and remediation actions taken.

FY2016 FISMA 2014 Reporting Metrics and the CSF

- ✓ For the first time, FISMA reporting metrics are organized around the NIST Framework for Improving Critical Infrastructure Cybersecurity, aka Cybersecurity Framework (CSF).

- ✓ The FY16 FISMA reporting metrics use CSF as a standard for managing/reducing cybersecurity risks, and are organized around the framework's five functions: Identify, Protect, Detect, Respond, and Recover.

- ✓ The CSF, in conjunction with NIST's *Guide for Applying the Risk Management Framework to Federal Information Systems* (SP 800-37), along with associated standards and guidelines, provides D/As with a structure for making ***more informed risk-based decisions*** and managing enterprise-wide cyber risks.

NIST Cyber Security Framework

CSF Anatomy

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2,

FY 2016 CIO FISMA Reporting Metrics

1. IDENTIFY: Goal of Identify metrics is to assist D/As with their inventory of GFE and other HW and SW systems and assets which are connected to their networks. Identification of these helps facilitate cybersecurity risk mgmt of the systems, assets, data & capabilities. CDM solutions should allow agencies to automatically detect and inventory many of these systems & assets.

1.1 For each FIPS 199 level, # of operational UNCLAS info systems by organization at that level: GOGO, GOCO, COCO, ATO, OA

1.2-1.5 # HW assets – all environments

1.6 IR policy in place

1.7 All contract with sensitive info contain clauses on protection/ detection/reporting of info IAW OMB guidance

1.8 Review of contracts with sensitive info is completed

1.9 Using FedRAMP-approved cloud services

Source: FY2016 CIO FISMA Metrics, V 1.0 1 October 2015

FY 2016 CIO FISMA Reporting Metrics

2. PROTECT: Goal of the Protect metrics are to ensure D/As safeguard their systems, networks, and facilities with appropriate cybersecurity defenses. Protect function supports ability to limit or contain impact of potential cybersecurity events.

2.1 % of UNCLAS networks w/capability to block unauthorized devices from connecting

2.2 % of UNCLAS networks with vulnerabilities assessments using SCAP validated products

2.4 Unprivileged Network Users

2.5 Privileged Network Users

2.6-2.8 Network Accounts

2.9-2.12 Least Privilege

2.13 Physical Access Control Systems

2.15-2.16 Data Protection and Remote Access (PIV/NIST LOA 4)

Source: FY2016 CIO FISMA Metrics, V 1.0 1 October 2015

FY 2016 CIO FISMA Reporting Metrics

3. DETECT: Goal of Detect metrics is to determine the extent to which D/As discover cybersecurity events in a timely manner. D/As should maintain and test intrusion-detection processes and procedures to ensure timely awareness of anomalous events on systems and networks.

3.1-3.6 Anti-Phishing Defense

3.7-3.11 Malware Defense

3.12-3.15 Other Defenses (capabilities beyond Anti-P & Malware)

3.16-3.22 Network Defense

- % of networks that implement unauthorized connection alerts
- # GFE endpoints and mobile assets covered by endpoint mgmt
- # Test exfiltration attempts caught
- Attempts to access large data volumes are detected/investigated
- All info security events are reported to US-CERT
- DHS Einstein 3A MOU/MOA signed
- Completed implementation of agency ISCM Dashboard or D/A Dashboard provided by CDM Program

Source: FY2016 CIO FISMA Metrics, V 1.0 1 October 2015

FY 2016 CIO FISMA Reporting Metrics

4. RESPOND: Goal of Respond metrics is to ensure D/As have policies and procedures that detail how their enterprise will respond to cybersecurity events. D/As should develop and test response plans and communicate response activities to stakeholders to minimize the impact of cybersecurity events, when they occur.

4.1 Date of last update to the Incident Response Plan

4.2 % of incidents vs. attempts that were successful

***For each of the following objectives, provide key completed activities and key planned activities on a quarterly basis*.**

4.3 Worst-case Incident Response Plan tested/updated within 30 days of test results

4.4 Establish partnership for surge resources and special capabilities

4.5 Roles and Responsibilities verified in incident response testing

4.6 Participation in Federal Cybersecurity Communication, Assessment, and Response (C-CAR) protocol

4.7 Incident Response Plan is at enterprise level, and developed and tested at least twice annually

Source: FY2016 CIO FISMA Metrics, V 1.0 1 October 2015

FY 2016 CIO FISMA Reporting Metrics

5. RECOVER: Goal of Respond metrics is to ensure D/As develop and implement appropriate activities for resilience that allow for restoration of any capabilities/services that were impaired during a cyber event. The recover function reduces the impact of a cyber event.

5.1 Date of last update to the Recovery Plan

5.2 % of public/internal notifications that were conducted IAW relevant statute, OMB policy, or D/A policies

***For each of the following objectives, provide key completed activities and key planned activities on a quarterly basis*.**

5.3 Disaster Recover Plans (SP 800-34) covering human threat sources, including those impacting electronic info or physical data loss

5.4 Business Continuity Plans (SP 800-34) are in place and fully tested for all levels of relevant cyber-related events

Source: FY2016 CIO FISMA Metrics, V 1.0 1 October 2015

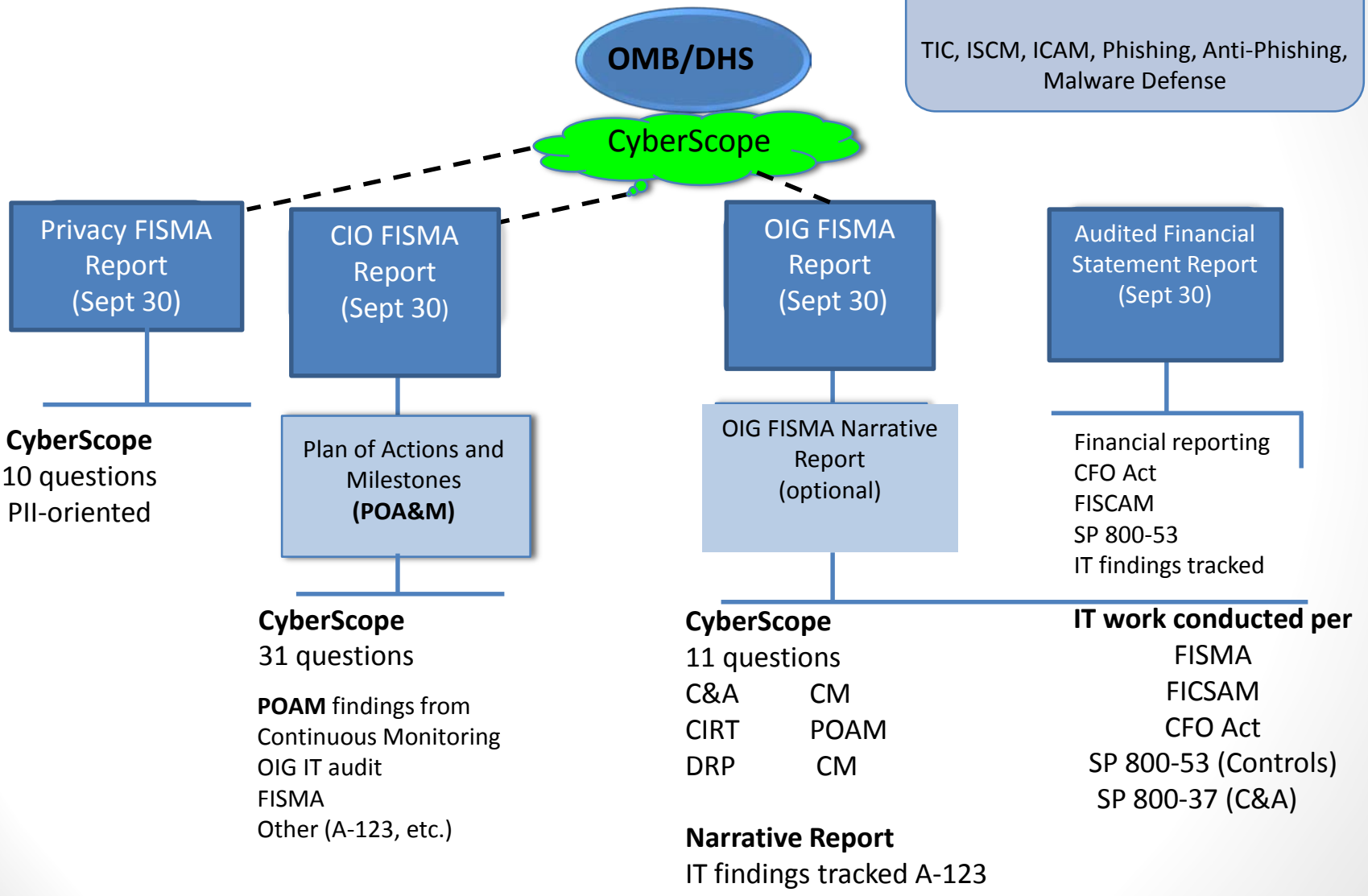
FY 2016 IG FISMA Reporting Metrics

- **Reporting Deadline:** November 10, 2016
- **Scoring:** Agencies are allotted points for each CSF Function area based on their achievement of various levels of 'maturity.' A total of 20 points is possible for each Framework Function.
- **Maturity Models: Full** (Detect and Respond) or **Indicators** (Identify, Protect, and Recover).

Cybersecurity Framework Security Functions	FY 2016 IG FISMA Metric Domains
Identify	Risk Management and Contractor Systems
Protect	Configuration Management, Identity and Access Management, and Security and Privacy Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

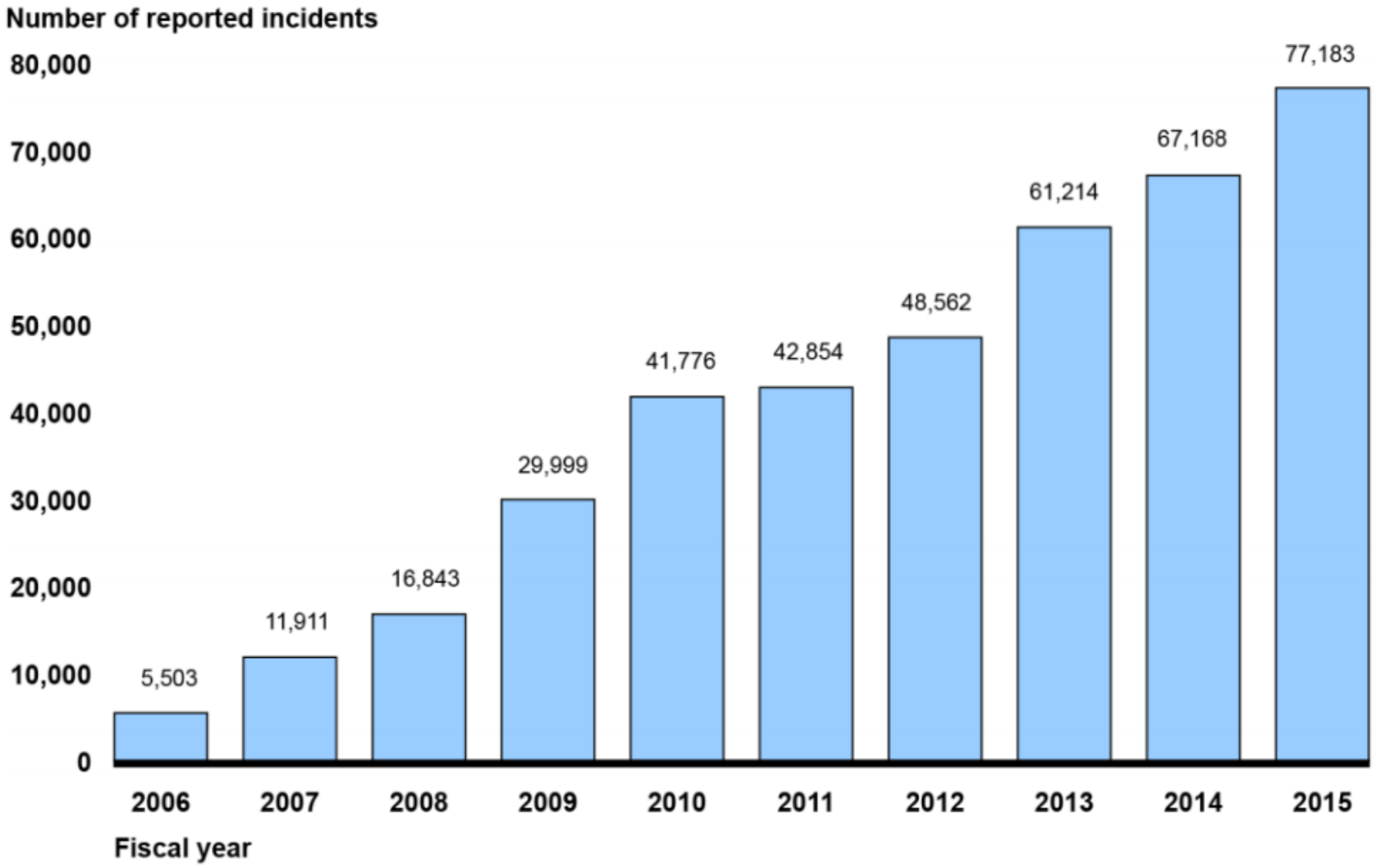
Source: FY 2016 Inspector General FISMA Reporting Metrics V1.1

FISMA & CAP Reporting



Source: Baker, Brett. OIG *Responsibilities under FISMA*, Information Security and Privacy Advisory Board, IG Panel, June 10, 2015.

Incidents Reported by Federal Agencies FY 2006-2015



Source: GAO analysis of the US CERT and OMB data for FY 2006-2015. (GAO-16-501)

Great need for Cybersecurity Metrics…

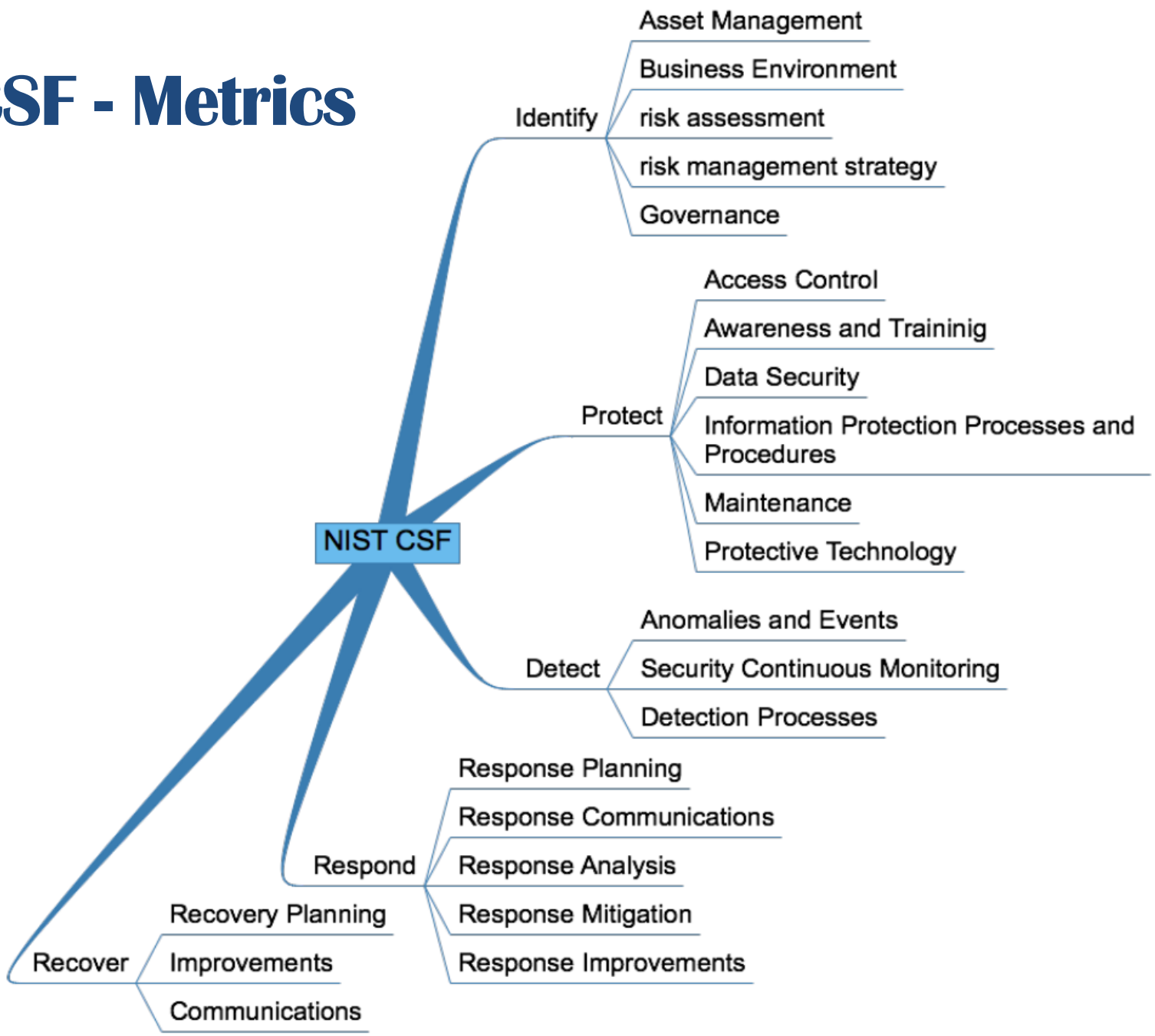
How to Measure Anything in Cybersecurity Risk. **Douglas W. Hubbard, Richard Seiersen, Daniel E. Geer, Jr. (Foreword), Stuart McClure (Foreword). July 2016**

The Truth about Cyber Risk Metrics Connecting Vulnerabilities to Economics, **Scott Borg, U.S. Cyber Consequences Unit, RSA Conference, April 2015.**

Cookin' Up Metrics With Alex and David: A Recipe For Success! **By Alexander Hutton, Society of Information Risk Analysts (SIRA), David Mortman, Chief Security Architect, Dell Software Group. RSA Conference, April 2015.**

The Failure of Risk Management: Why It's Broken and How to Fix It. **Douglas W. Hubbard. April 2009, John Wiley & Sons.**

CSF - Metrics



Source: Society of Information Risk Managers - https://societyinforisk.org

Cybersecurity National Action Plan (CNAP)

CNAP – Government-Focused Initiatives

- ✓ **The Federal Privacy Council (FPC).** Composed of Chief Privacy Officers of agencies across the government. FPC will function similarly to existing CIO Council, as a convening and coordinating body for harmonization of policies and best practices across government.

- ✓ **New Federal Chief Information Security Officer (CISO) position.**

- ✓ **$3.1 billion for Information Technology Modernization Fund** Hope to eliminate/avoid infrastructure challenges that caused vulnerabilities leading to major breaches at OPM, Interior, etc.

- ✓ **Decreasing reliance on Social Security Numbers** for identification

- ✓ **Use of identity proofing and strong multi-factor authentication**

CNAP Programs

- ✓ **The Commission on Enhancing National Cybersecurity.** 12 members of private sector have been meeting monthly since April. Their goal is to recommend public and private sector actions to strengthen cybersecurity over the next 10 years. Recently posted an RFI asking for ideas on a range of cybersecurity issues, from IOT to cyber insurance. Final report submitted to the President: Dec. 1.

- ✓ **National Cybersecurity Awareness Campaign, Use of Multifactor Authentication.** Campaign to provide consumers with education on hardening strategies, such as multifactor authentication to secure online accounts. Calls on companies to enable multifactor authentication for their users.

- ✓ **Cybersecurity Assurance Program**. DHS will work with industry partners to create a security certification program for networked devices, i.e., "CyberUL."

CNAP Programs

- ✓ **National Center for Cybersecurity Resilience.** Opened in Rockville February 2016, supported by DHS, Commerce and DOE. Will allow companies and sector-wide organizations to test security of systems in a contained environment.

- ✓ **Enhance Cybersecurity Education and Training.** Includes the Cybersecurity Core Curriculum, designed to prep graduates who want to work cyber positions in the Federal Government.

- ✓ **Strengthening Internet 'Utilities.'** Government and private sector organizations, such Linux Foundation's Core Infrastructure Initiative, to fund and secure open-source software, protocols, and standards, among other things.

- ✓ **CyberCorps Reserve program.** Increasing the number of DHS civilian cyber defense teams.

Resources

- Baker, Brett. OIG *Responsibilities under FISMA*, Information Security and Privacy Advisory Board, IG Panel, June 10, 2015. http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-06/ispab_june-10_fisma_bbaker.pdf

- The Commission on Enhancing National Cybersecurity
  Meetings: http://www.nist.gov/cybercommission/commission-meetings.cfm
  RFI: http://www.nist.gov/cybercommission/cybercommission-rfis.cfm

- *Cookin' Up Metrics With Alex and David: A Recipe For Success!* By Alexander Hutton, Society of Information Risk Analysts (SIRA), David Mortman, Chief Security Architect, Dell Software Group. RSA Conference, April 2015. https://www.rsaconference.com/events/us15/agenda/sessions/1601/cookin-up-metrics-with-alex-and-david-a-recipe-for

- FEDERAL INFORMATION SECURITY:*Agencies Need to Correct Weaknesses and Fully Implement Security Programs* GAO-15-714: Published: Sep 29, 2015.

- Global Forum to Advance Cyber Resilience. https://gfacr.org/2016/05/18/nist-cyber-security-framework-2/

Resources

- *How to Measure Anything in Cybersecurity Risk.* Douglas W. Hubbard, Richard Seiersen, Daniel E. Geer, Jr. (Foreword), Stuart McClure. July 2016
- ISSA Northern Virginia Chapter (NOVA) - http://nova.issa.org/
- ISSA-NOVA SIG RMF Lifeboat Meetup - https://www.meetup.com/NCR-Risk-Management-Framework-Lifeboat/events/past/?scroll=true#past
- NIST Cybersecurity Framework – www.nist.gov/cyberframework
- Society of Information Risk Managers - https://societyinforisk.org
- The Cartoonist Group - http://www.cartoonistgroup.com
- *The Failure of Risk Management: Why It's Broken and How to Fix It*. Douglas W. Hubbard. April 2009, John Wiley & Sons.
- *THE US CYBER SECURITY MATRIX:* A New Type of Check List for Defending Against Cyber Attacks, by Scott Borg and John Bumgarner, US Cyber Consequences Unit (a 501C3). http://www.usccu.us/

Questions?