The Evolution of Cybersecurity Auditing

Presented to:

NIAF Cybersecurity Forum

July 19, 2017

The Evolution of Cybersecurity Auditing

I. The Early Years: Building awareness, capacity, methodologies, and infrastructure (Bob Dacey)

II. Auditing IT Security: Using a risk-based approach (Greg Wilshusen)

III. What's Next: NIST's cybersecurity framework, maturity models, and more (Naba Barkakati)

The Early Years: Building Awareness, Capacity, Methodologies, and Infrastructure

Robert Dacey Chief Accountant
202.512.7439 – daceyr@gao.gov

NIAF Cybersecurity Forum -- July 19, 2017

Early recognition of importance of cybersecurity and scope of issue

- In 1993, began increasing focus on assessing computer security
- Incorporated examination of information security over financial systems as part of financial audits in *Financial Audit Manual*
- Hired additional information security specialists and contracted penetration testing as part of financial audits
- Recognized early on that the scope of cybersecurity issues extended beyond government systems to systems in the private sector and systems supporting critical infrastructure.
- Expanded our audit scope to include agency information security programs, cyber critical infrastructure protection, emerging technologies (such as mobile devices, wireless, embedded medical devices).
- With constant revelation of successful cyber attacks, cybersecurity continues to be a major concern of both the government and the private sector

Strategy for Cybersecurity Audits (1997)

1. Build capacity

- Expanded cadre of IT security auditors and specialists
- Created an e-security lab to develop and test new audit techniques and hone skills of IT specialists
- Established Joint Information Security Audit Initiative to cooperatively work with the state and local audit community to build information security audit capacity and increase awareness of information security risks (2001)

2. Develop common methodology & leverage resources across government

- Studied the practices of leading organizations with superior security programs to identify fundamental risk management principles and best practices
- Developed FISCAM (Federal Information System Controls Audit Manual) to guide information security audits.
- Leveraged resources across government by engaging agency Inspectors General to conduct computer security audits in accordance with FISCAM
- Developed a risk-based approach to cybersecurity, that has remained a bedrock principle of cybersecurity in U.S. government to this day

3. Work with Congress to build and refine legislative framework

Raised Congressional awareness of pervasive computer security weaknesses across government through our audit reports and high-risk list

- Designated information security as a government-wide high-risk area in 1997 (20th anniversary)
- Expanded the cybersecurity high-risk area to include the protection of critical cyber infrastructure in 2003.
- Further expanded the high-risk area to include protecting the privacy of personally identifiable information in 2015.

3. Work with Congress to build and refine legislative framework

- Helped to facilitate the development and passage of FISMA (Federal Information Security Management Act) in 2002. The law codified a comprehensive risk-based framework for securing federal information systems. FISMA:
  - required federal agencies to implement entity-wide information security programs that incorporate elements of GAO's best practices work
  - resulted in the development of a body of government security standards and guidelines by NIST
  - provided an accountability mechanism by requiring agency Inspectors General and GAO to evaluate and report on agency compliance

3. Work with Congress to build and refine legislative framework

- Numerous reports and testimonies to inform Congress on agencies' cybersecurity, including implementation of FISMA requirements, government-wide assessment, specific agency assessments, and analysis specific security issues (e.g., industrial control systems)

Auditing IT Security: Using a Risk-Based Approach

Greg Wilshusen, Director, Information Security Issues
202.512.6244 – wilshuseng@gao.gov

NIAF Cybersecurity Forum -- July 19, 2017

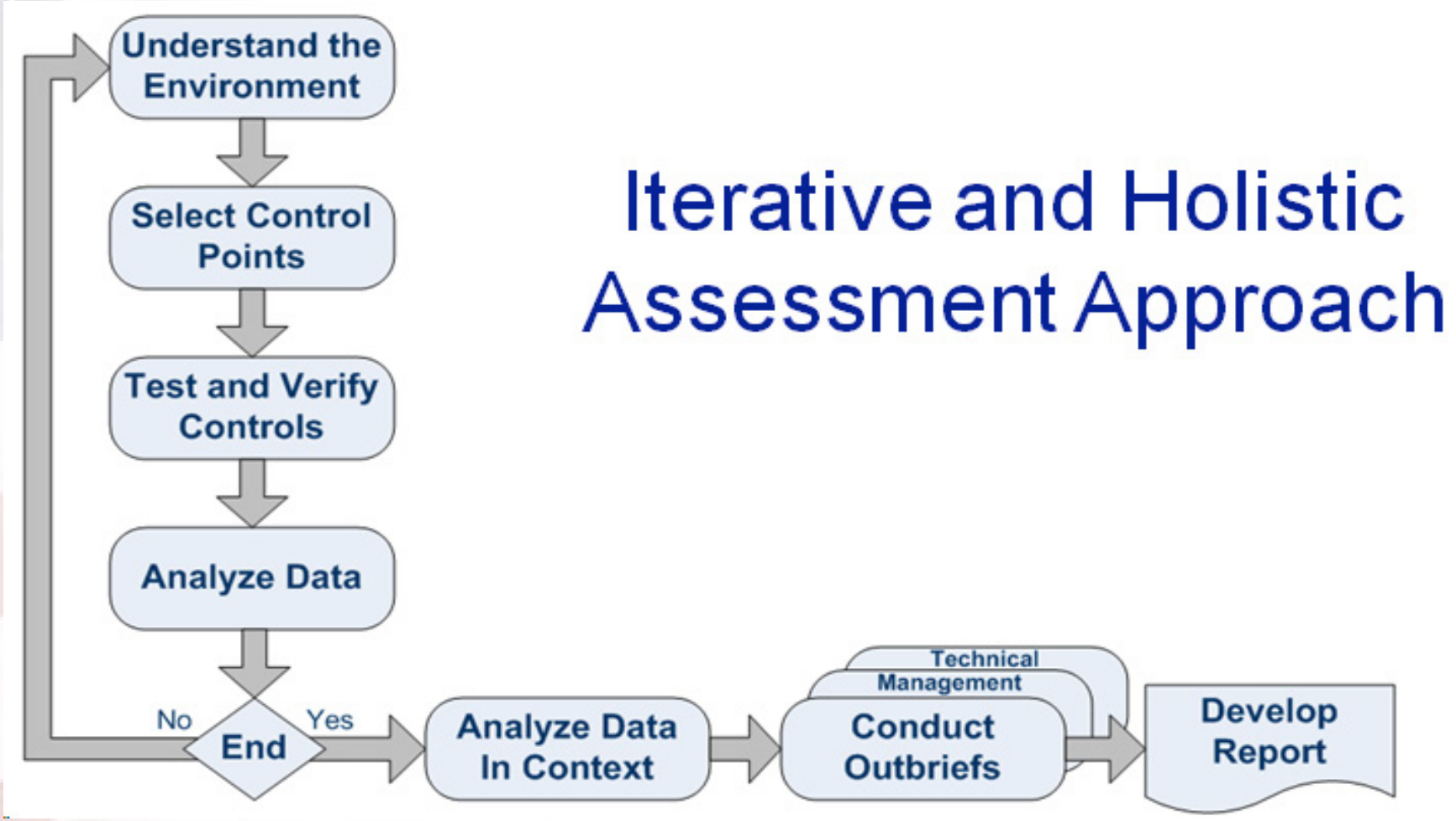
GAO audit methodology for assessing IT security controls

- *Federal Information System Controls Audit Manual* (GAO-09-232G)
- Objective: To assess effectiveness of agency's security controls in protecting the confidentiality, integrity, and availability of its information systems and information.
- Control Categories:
  - Access controls -- Physical and Logical
  - Configuration management
  - Segregation of duties
  - Contingency planning
  - Security management

Criteria for IT Security Audits

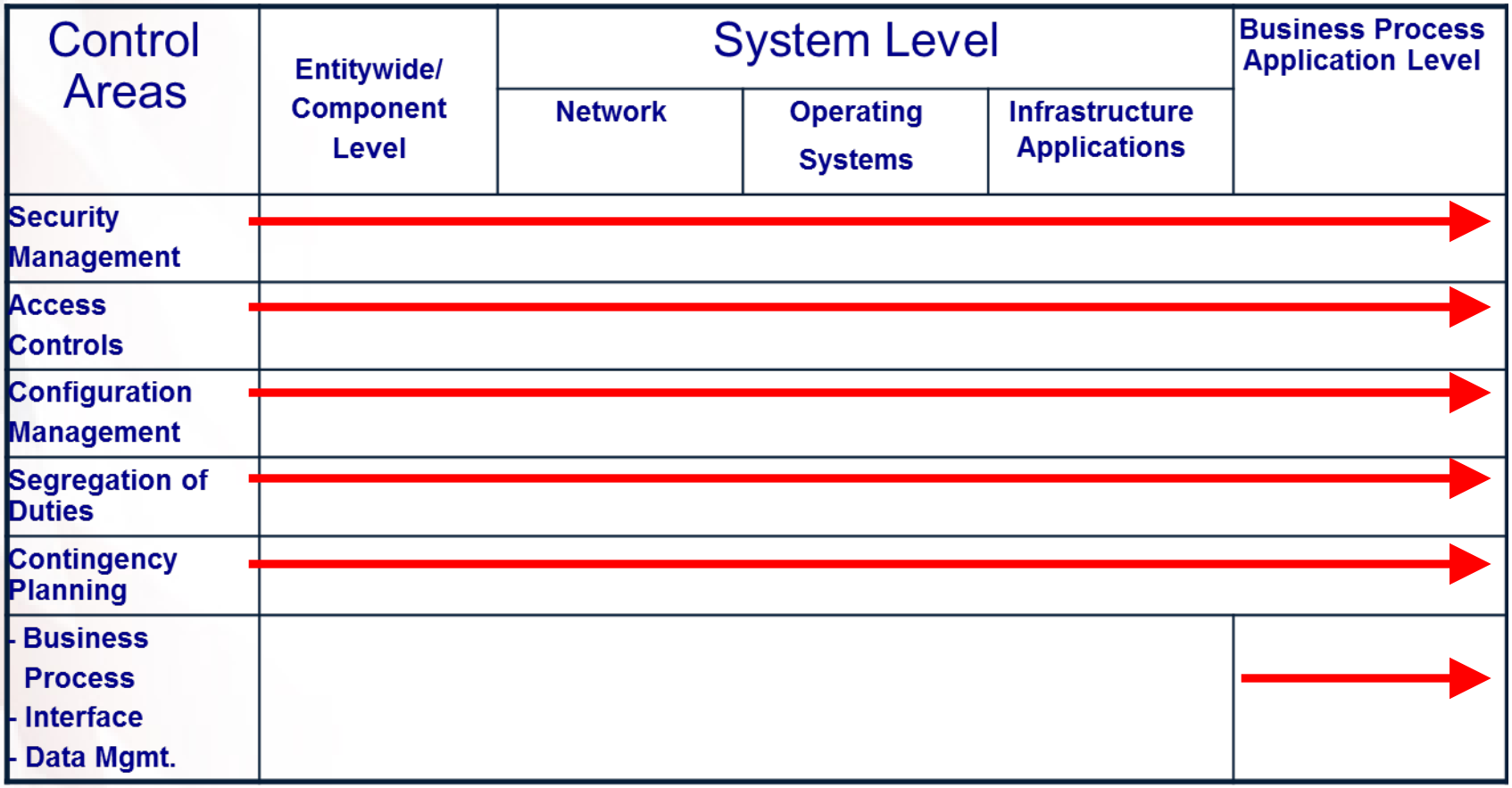
- *Federal Information Security Modernization Act of 2014*
- *Cybersecurity Act of 2015*
- OMB Memoranda
- DHS Binding Operational Directives
- NIST Federal Information Processing Standards and SP 800-series
- US Government Configuration Baselines
- DISA *Security Technical Implementation Guides* (STIGs)
- Vendor Security Guidelines
- GAO's *Standards for Internal Control in the Federal Government*

Overall audit process

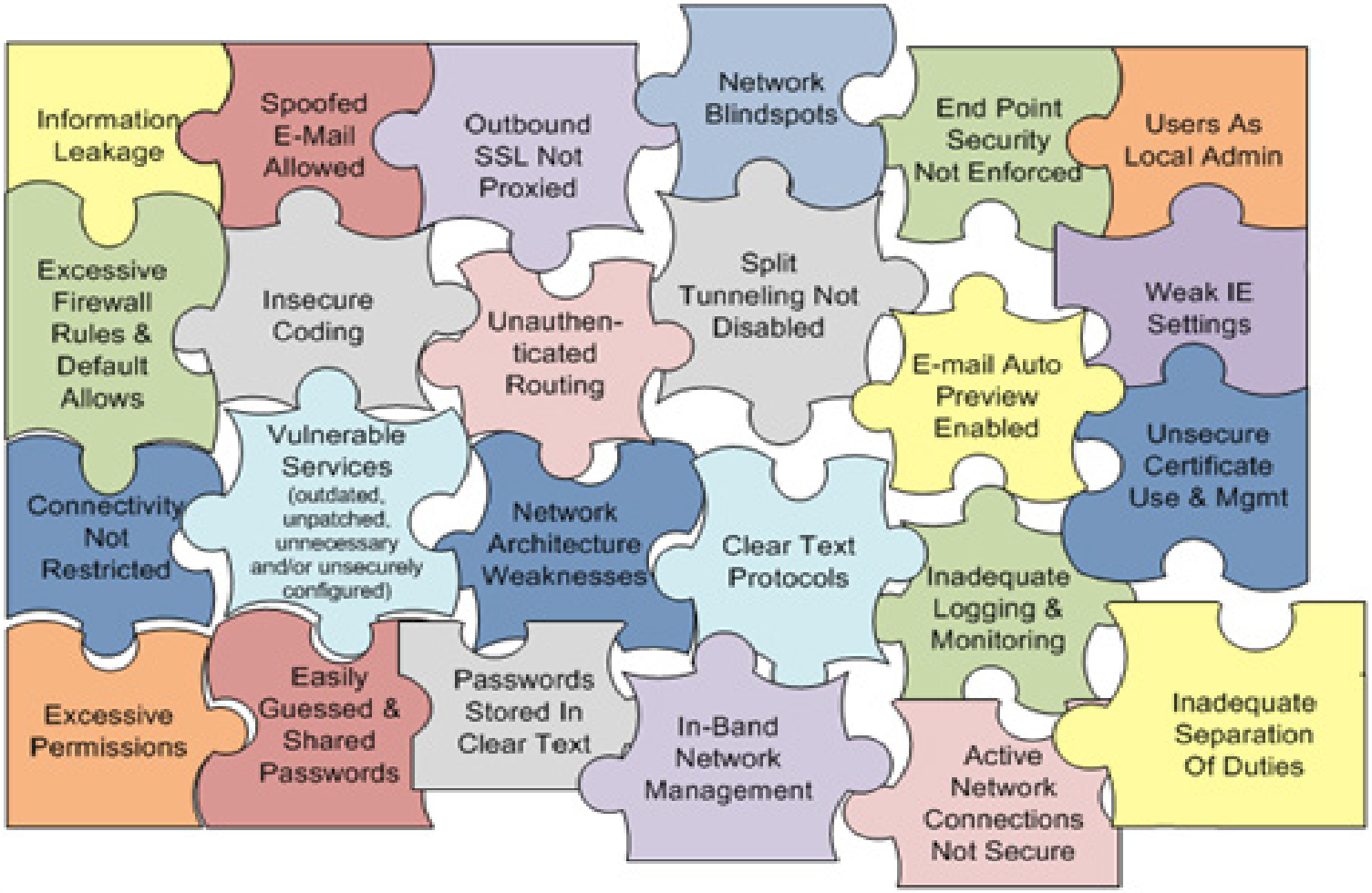


Iterative and Holistic Assessment Approach

Assessing control areas by level



Assess significance of findings

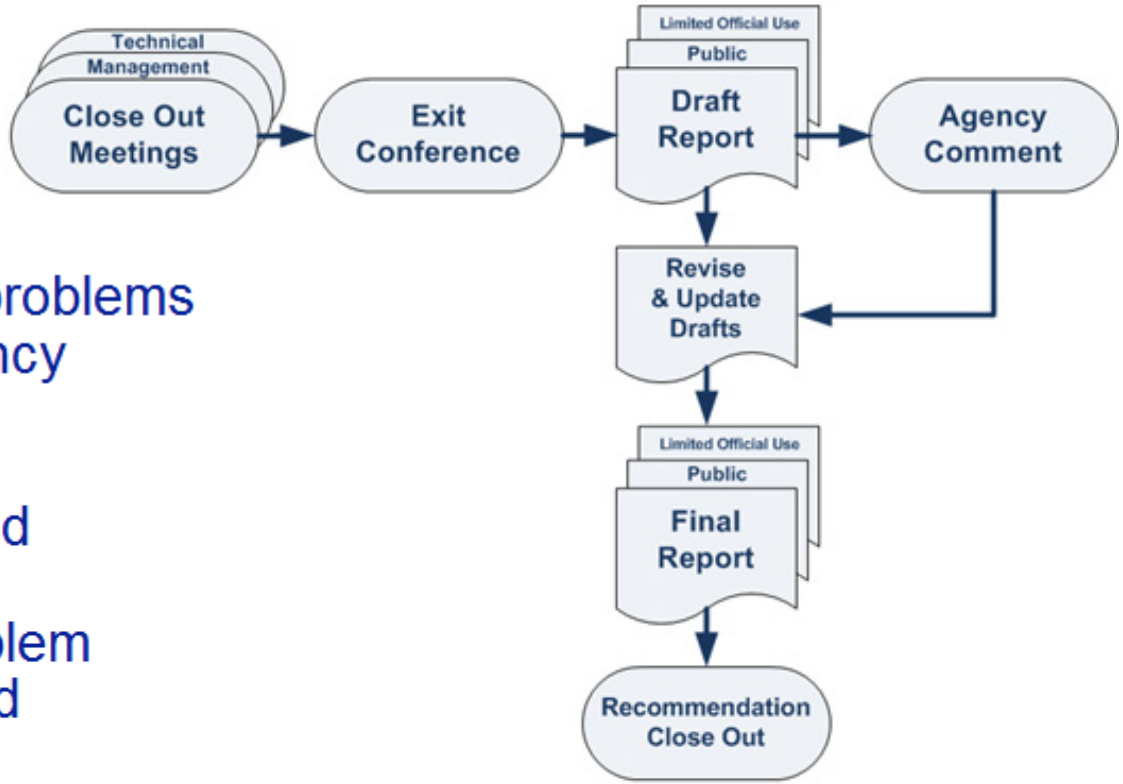


Assess vulnerabilities in the context of the network connectivity and the impact on the organization's mission.

Examine Agency IT Security Processes

- Assessing cyber risks
- Selecting and documenting IT security controls
- Providing security training
- Monitoring, testing, and evaluating controls
- Detecting, responding, and recovering from incidents
- Mitigating vulnerabilities
- Overseeing contractors

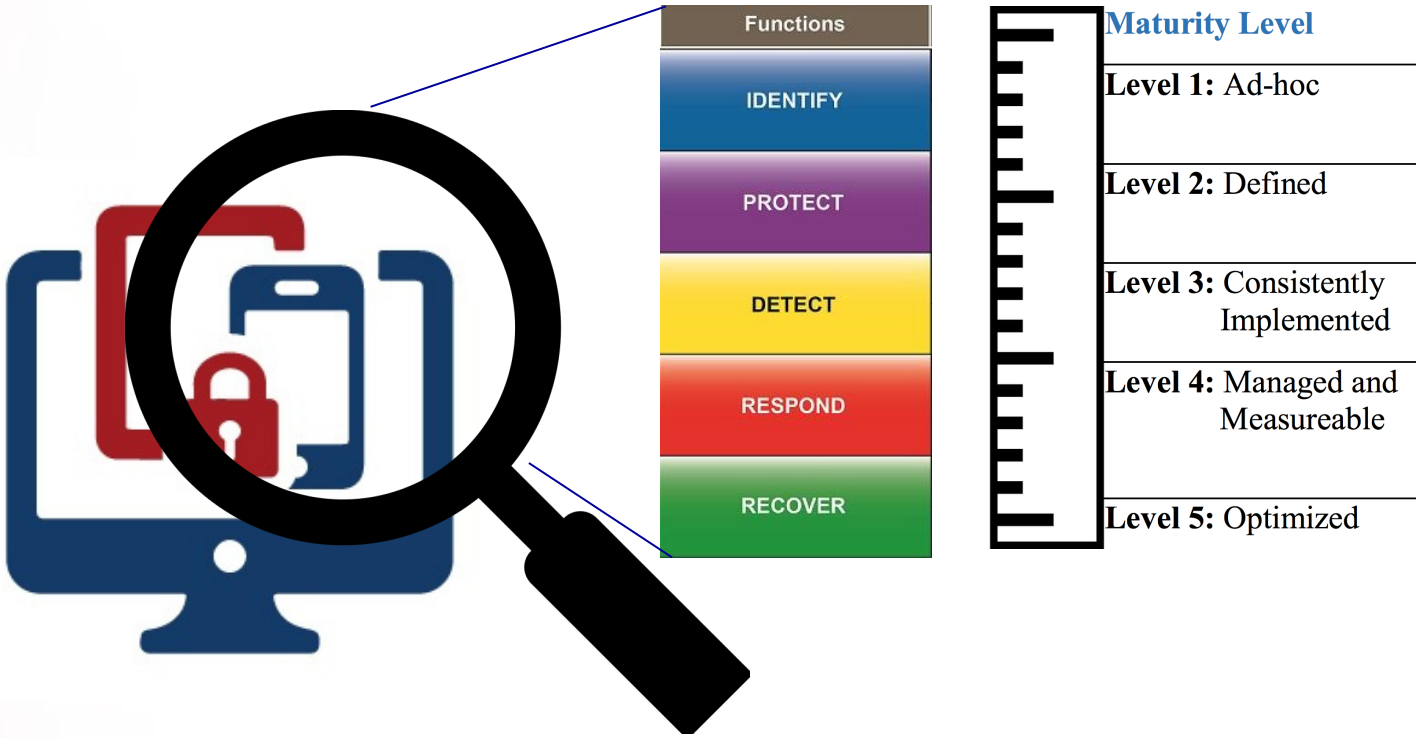
Communicating results of audit



Focus on most important problems – the ones that'll help agency become more secure

Criteria – NIST, vendor and industry guidance
Condition – describe problem
Effect – explain what could happen if exploited
Cause – sometimes unclear, often related to immature information security program

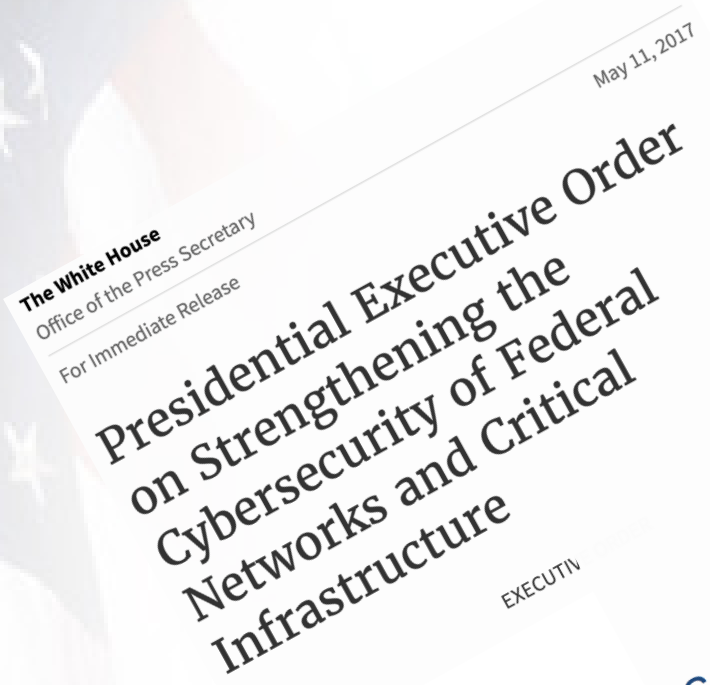
What's Next: NIST Cybersecurity Framework, Maturity Levels, and More



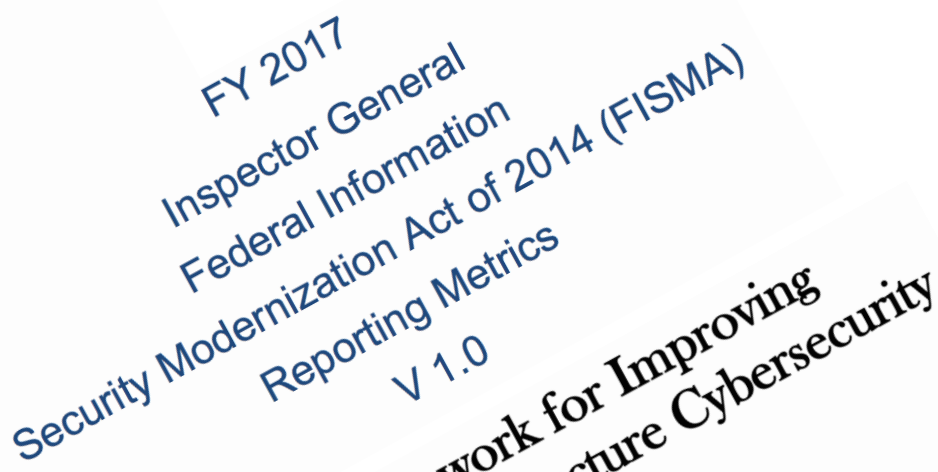
Naba Barkakati, Ph.D, Chief Technologist
202.512.4499 – barkakatin@gao.gov

NIAF Cybersecurity Forum -- July 19, 2017

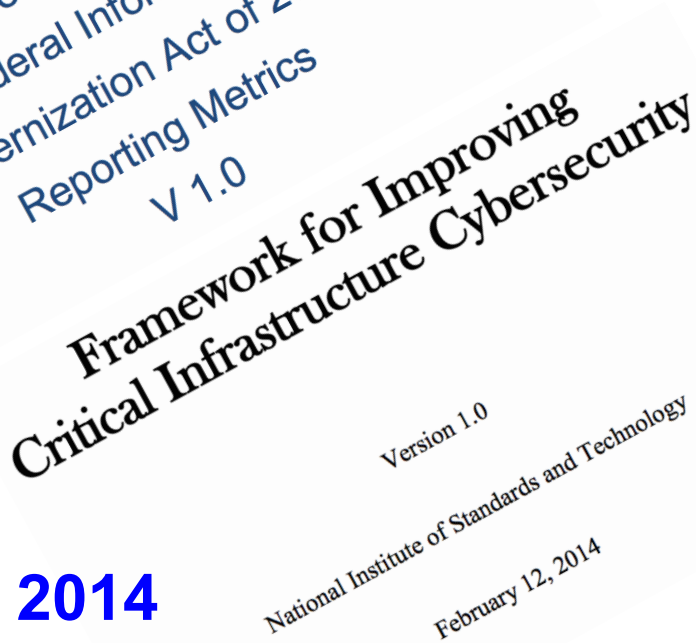
Recent cybersecurity items of interest...



May 2017



April 2017



Feb 2014

NIST Cybersecurity Framework (CSF)

Component	Description
Framework Core	5 concurrent and continuous Functions — Identify, Protect, Detect, Respond, Recover. with associated activities, desired outcomes, and applicable references
Framework Implementation Tiers	4 Tiers: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4) that describe the degree to which an organization's practices exhibit characteristics defined in the Framework
Framework Profiles	Represents outcomes based on business needs. Used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state)

NIST Framework for Improving Critical Infrastructure Cybersecurity, (v 1.0, Feb 2014, draft v1.1 Jan 2017) https://www.nist.gov/cyberframework

Core Functions and Categories

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

Using the NIST CSF

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8

What to Do

Information that can help to achieve it

Seven step process to implement a cybersecurity program

Step 1: Prioritize and Scope

Step 2: Orient

Step 3: Create a Current Profile

Step 4: Conduct a Risk Assessment

Step 5: Create a Target Profile

Step 6: Determine, Analyze, and Prioritize Gaps

Step 7: Implement Action Plan

IG FISMA metrics aligned with NIST CSF

Table 1: IG and CIO Metrics Align Across NIST Cybersecurity Framework Function Levels

Function (Domains)	IG Metrics	CIO Metrics
Identify (Risk Management)	X	N/A
Protect (Configuration Management)	X	X
Protect (Identity and Access Management)	X	X
Protect (Security Training)	X	X
Detect (Information Security Continuous Monitoring)	X	X
Respond (Incident Response)	X	X
Recover (Contingency Planning)	X	X

IGs to assess effectiveness of information security programs using five maturity model levels: Ad-hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

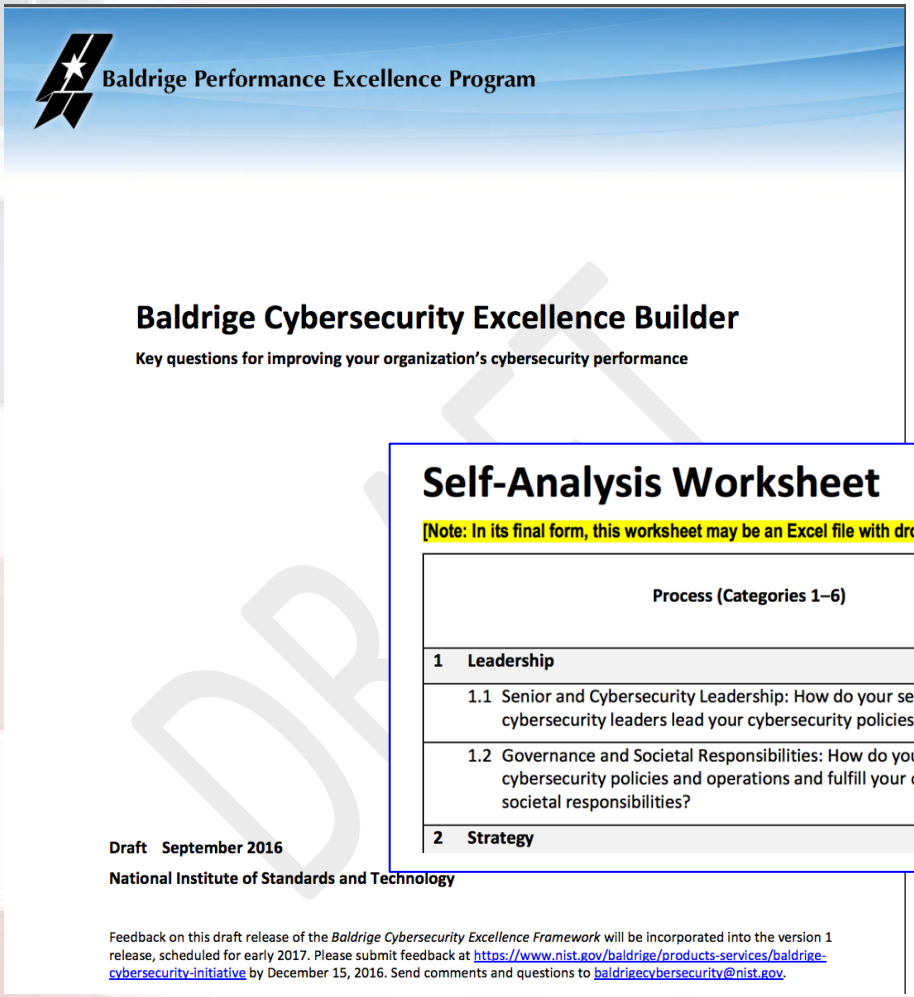
Level 4, Managed and Measurable, represents an effective level of security.

Table 2: IG Assessment Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measureable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

DHSFY17 FISMA Documents, https://www.dhs.gov/publication/fy17-fisma-documents

NIST releases draft self-assessment tool for cybersecurity excellence



Baldrige Performance Excellence Program

Baldrige Cybersecurity Excellence Builder

Key questions for improving your organization's cybersecurity performance

Draft September 2016

National Institute of Standards and Technology

Feedback on this draft release of the *Baldrige Cybersecurity Excellence Framework* will be incorporated into the version 1 release, scheduled for early 2017. Please submit feedback at https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative by December 15, 2016. Send comments and questions to baldrigecybersecurity@nist.gov.

Self-Analysis Worksheet

[Note: In its final form, this worksheet may be an Excel file with drop-down boxes and/or another type of non-paper-based tool.]

Process (Categories 1–6)	Reactive, Early, Mature, or Role Model?				High, Medium, or Low?
	Approach	Deployment	Learning	Integration	Importance
1 Leadership					
1.1 Senior and Cybersecurity Leadership: How do your senior and cybersecurity leaders lead your cybersecurity policies and operations?					
1.2 Governance and Societal Responsibilities: How do you govern your cybersecurity policies and operations and fulfill your organization's societal responsibilities?					
2 Strategy					

- Tool based on Baldrige Excellence Framework - draft released Sep 2016
- Helps organizations better understand the effectiveness of their cybersecurity risk management efforts
- Includes self-assessment rubric with maturity levels that enables organizations to measure how effectively they are using the Cybersecurity Framework

Baldrige Cybersecurity Excellence Builder, NIST, draft September 2016
https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf

Panelists

Moderator:

- Tammy Whitcomb, Acting Inspector General, U.S. Postal Service; Committee Chair, CIGIE Information Technology Committee

Discussants:

- Robert Dacey, Chief Accountant, U.S. GAO, 202-512-7439, daceyr@gao.gov
- Naba Barkakati, Chief Technologist, U.S. GAO, 202-512-4499, barkakatin@gao.gov
- Greg Wilshusen, Director, Information Security Issues, U.S. GAO, 202-512-6244, wilshuseng@gao.gov