

# How did we get here and what's next?

May 9, 2019





#### **Glenn Keaveny**

Director National Advisory Services Public Sector | Risk Advisory Services T: 703-562-5946 glenn.keaveny@us.gt.com





# **Learning Objectives**

- NIST History
- Tools and Techniques to Operate Under Current Standards and Conditions
- What Does the Future Look Like?
- What to do Now to be Ready for Tomorrow



# Agenda

- NIST History (Why NIST?)
- NIST Mission
- Frameworks
- Tools and Techniques
  - First Things First (Implementation and Remediation)
  - Not My Problem (Inheritance)
  - Reciprocity
- The NIST Horizon
- What to do Now
- Questions



# Why NIST?





# Why NIST?

#### DOJ Breach Overshadows New Cybersecurity Plan

In the wake of another federal data breach, the president hopes for a cybersecurity funding boost and unveils an action plan.

### ARMY NATIONAL GUARD HIT WITH DATA BREACH

IRS sued over data breach that affected 330,000 people

SPONSORED BY The Morning Download: Intruders Hit DHS, Justice as White House Calls for Bigger Cybersecurity Budget By Steve Rosenbush Obama unveils national cybersecurity action plan and budget

Federal officials grapple with response to data breaches

### About Those Fingerprints Stolen in the OPM Hack

The federal agency said Wednesday it underestimated the number of people whose fingerprints were exposed in a massive data breach.

### Exclusive: The OPM breach details you haven't seen

antThornton

An official timeline of the Office of Personnel Management breach obtained by FCW pinpoints the hackers' calibrated extraction of data, and the government's step-by-step response.

# Why NIST?

IBM-Ponemon Study

•

- The average cost incurred for each lost or stolen record containing sensitive and confidential information increased from **\$154** to **\$158**. Similar numbers show that in 2014 that number was **\$145** 
  - o Loss of reputation difficult to quantify
  - Leaks: Unprecedented leaks of comprehensive datasets, with over 4 billion compromised records exposed.
  - Methods: Cybercriminals continue to favor older attack methods to gain access to valuable data and resources, including command injection, malware and ransomware.





## **NIST History**





# **NIST History**

- 1821 "Weights and measures may be ranked among the necessities of life to every individual human society" – John Quincy Adams
- 1830-1901 The Office of Standard Weights and Measures
- 1838 The United States establishes a uniform standard of weights and measures
- 1901 National Bureau of Standards is established to provide standard weights and measures and serve as the national physical laboratory
  - Meteorological Services
  - Expands Weights and Measures (Materials, Light, Electricity)
- 1988 National Institute of Standards and Technology (NIST)
  - Promote U.S. innovation and industrial competitiveness by advancing <u>measurement science</u>, <u>standards</u>, and <u>technology</u> in ways that enhance economic security and improve our <u>guality of life</u>.



## **NIST History**





### **Frameworks**

- NIST has 1,102 Cybersecurity Publications
  - NIST SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems a: A Security Life Cycle Approach (RMF)
    - NIST SP 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Information
    - NIST SP 800-171, Revision 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
  - Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (CSF)
  - Federal Risk and Authorization Management Program (FedRAMP)





### **Risk Management Framework**





### RMF

- The risk-based approach to risk management considers:
  - organization-wide risk
  - integration of activities into the system development life cycle (SDLC)
    - Will be discussed next slide
  - considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations.

Applicable NIST Publications:

- NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-37 Rev 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800-30 Rev 1 Guide for Conducting Risk Assessments
- NIST SP 800-160 System Security Engineering



### CSF

#### • NIST Cybersecurity Framework – Overview

- Executive Order 13631 (Feb. 2013) Directed a "Framework for Improving Critical Infrastructure Cybersecurity"
  - NIST to lead creation of Framework working with stakeholders from industry, government, and academia
  - Prioritized, risk-based, include performance measures, etc.
  - Identify and leverage established cybersecurity standards, guidelines, and practices
- Final NIST CSF v1.1
- Components of NIST CSF
  - Framework Tiers
  - Framework Profiles Current vs. Target
  - Framework Core



### **CSF** Tiers





### **CSF** Profiles







**v †** 

| C      | Cybersecurity Profile |
|--------|-----------------------|
| SN     | IDENTIFY D            |
| INCTIO | protect PR            |
| DRK FU | detect DE             |
| AMEWO  | RESPOND RS            |
| FR     | RECOVER RC            |



### **CSF** Core

|          | Function     |   | Category  | Subcategory  |  |  |  |  |
|----------|--------------|---|---|--|--|--|--|--|
| IDENTIFY | (ID)         | Asset Managemen<br>Business Environn<br>Governance (ID.G<br>Bisk Assessment)  | nent (ID.BE)  | Access Control (PR.AC)<br>PR.AC-1: Identities and credentials are  |  |  |  |  |
|          | Function     | Category  | Subcategory   | Informative References   |  |  |  |  |
| PROTEC1  | PROTECT (PR) | Access Control (PR.AC): Access to assets<br>and associated facilities is limited to<br>authorized users, processes, or devices, and to<br>authorized activities and transactions. | <b>PR.AC-1</b> : Identities and credentials are maged<br>authorized devices and users                                   | <ul> <li>CIS Controls v7 16</li> <li>COBIT 5 DSS05.04, DSS06.03</li> <li>for 'ISA 02443-2-12009 4.3.3.5.1</li> <li>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9</li> <li>ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3</li> </ul> |  |  |  |  |
| DETECT ( |              |   | PR.AC-2: Physical access to assets is managed a protected   | KuS1 SF 500-55 Rev. 4 AC-2, IA ramay     COBIT 5 DSS01.04, DSS05.05     ISA 62443-2-1:2009 4.3.3.3.8     ISO/IEC 27001:2013 A.11.1.4, A.11.1.6, A.11.2.3     NOTE OF 000-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9  |  |  |  |  |
| RESPON   |              |   | PR.AC-3: Remote access is managed   | COBIT 5 APO13.01, DSS01.04, DSS05.03     ISA 62443-3-1:2009 4.3.3.6.6     ISA 62443-3-3:2013 SR 1.13, SR 2.6     ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1     NIET 5P 909 53 Rev. 4 AC 17, AC 19, AC 20  |  |  |  |  |
| RECOVEF  |              |   | PR.AC-4: Access permissions are managed,<br>incorporating the principles of least privilege and<br>separation of duties | <ul> <li>CIS Controls v7 12, 13</li> <li>ISA 62443-2-1:2009 43.3.7.3</li> <li>ISA 62443-3-3:2013 SR 2.1</li> <li>ISO/IEC 27001:2013 A.6.12, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4</li> <li>NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16</li> </ul>   |  |  |  |  |
|          |              |   | PR.AC-5: Network integrity is protected,<br>incorporating network segregation where appropri                            | • ISA 62443-2-1:2009 4.3.3.4           • ISA 62443-3-3:2013 SR 3.1, SR 3.8           ate         • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1           • NIST SP 800-53 Rev. 4 AC-4, SC-7  |  |  |  |  |



#### The Federal Risk and Authorization Management Program (FedRAMP)

- Developed in collaboration with NIST, GSA, DOD, NSA, OMB, CIO Council, DHS, and private industry
- Mandated by OMB Memo on December 8, 2011
- Requires assessment of a subset of NIST Special Publication 800-53 controls
- Standardizes security assessment, authorization, and continuous monitoring for cloud service providers (CSPs)
- Risk-based model that can be leveraged government-wide
- Provides processes, artifacts, and a secure repository that enables agencies to leverage authorization











- 1. Document: CSPs categorize the type of data; Select and implement security control baseline
- 2. Assess: Independent Assessor (IA) evaluates security controls
- **3. Authorize**: IA delivers Security Assessment Report (SAR); IA and CSP create Plane of Action and Milestones (POA&Ms)
- 4. Monitor: CSP enters the continuous monitoring phase





## **Tools and Techniques**

- First Things First!
  - Implementation Demo
  - Remediation Demo
- Not My Problem!
  - Inheritance Demo
- Reciprocity



## **The NIST Horizon**

NIST SP 800-37 Rev 2: Risk Management Framework for Information systems and Organizations: A System Lifecycle Approach for Security and Privacy

- Identify missions, business functions, and processes that will be supported by the system
- Define organizational risk management strategy
- Identify stakeholders

antThornton

- Conduct initial risk assessment and determine the value of organizational assets
- Define stakeholder protection needs and security requirements
- Determine system boundaries
- Identify how the system integrates into the enterprise and security architecture of the organization
- Identify and assign specific roles associated with RMF execution



Holistic approach tightens linkage and alignment to business mission

#### Integrated Framework for Privacy & Security

### **The NIST Horizon**

#### **Integrated Framework for Privacy & Security**





### NIST SP 800-53 Rev. 5

- Security and Privacy Controls for Information Systems and Organizations
- Expanded focus on supply chain, cloud, mobile, cyberphysical, industrial/process control systems, and IoT devices
- Outcome-based controls structure
- Full integration of privacy controls into the security control catalog
- Integration with the Cybersecurity Framework
- New controls based on threat intelligence and empirical attack data



### **NIST SP 800 53 Rev 5 Outcome-based control focus**

| Revision 4 control structure   | Revision 5 control structure   |
|--|--|
| SC-8 TRANSMISSION CONFIDENTIALITY AND<br>INTEGRITY   | SC-8 TRANSMISSION CONFIDENTIALITY AND<br>INTEGRITY   |
| <u>Control</u> : The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information. | <u>Control</u> : Protect the [Selection (one or more): confidentiality; integrity] of transmitted information. |
| IA-2 IDENTIFICATION AND AUTHENTICATION<br>(ORGANIZATIONAL USERS)   | IA-2 IDENTIFICATION AND AUTHENTICATION<br>(ORGANIZATIONAL USERS)   |
| <u>Control</u> : The information system implements multifactor authentication for network access to privileged accounts.               | <u>Control</u> : Implement multifactor authentication for network access to privileged accounts.               |



### NIST SP 800 53 Rev 5 – Privacy control Integration

#### TABLE E-2: AWARENESS AND TRAINING FAMILY

| CONTROL        |  | AWN | ELATED    | TED BY   | NCE    | CONTROL BASELINES |     |      |
|----------------|--|-----|-----------|----------|--------|-------------------|-----|------|
| NUMBER         | CONTROL NAME<br>CONTROL ENHANCEMENT NAME                   |     | PRIVACY-R | IMPLEMEN | ASSURA | LOW               | MOD | HIGH |
| <u>AT-1</u>    | Awareness and Training Policy and<br>Procedures            |     | Р         | 0        | A      | х                 | x   | x    |
| <u>AT-2</u>    | Awareness Training   |     | Р         | 0        | А      | х                 | х   | х    |
| AT-2(1)        | PRACTICAL EXERCISES  |     | Р         | 0        | А      |                   |     |      |
| AT-2(2)        | INSIDER THREAT   |     |           | 0        | А      |                   | х   | х    |
| AT-2(3)        | SOCIAL ENGINEERING AND MINING                              |     |           | 0        | А      |                   | х   | х    |
| <u>AT-3</u>    | Role-Based Training  |     | Р         | 0        | А      | х                 | х   | х    |
| AT-3(1)        | ENVIRONMENTAL CONTROLS                                     |     |           | 0        | А      |                   |     |      |
| AT-3(2)        | PHYSICAL SECURITY CONTROLS                                 |     |           | 0        | А      |                   |     |      |
| AT-3(3)        | PRACTICAL EXERCISES  |     | Р         | 0        | А      |                   |     |      |
| <u>AT-3(4)</u> | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS<br>SYSTEM BEHAVIOR |     |           | 0        | А      |                   |     |      |



### NIST SP 800 53 Rev 5 – Privacy Control Integration

| <u>IP-1</u>    | Individual Participation Policies and Procedures              | Р | R |
|----------------|---|---|---|
| <u>IP-2</u>    | Consent   | Ρ | S |
| <u>IP-2(1)</u> | Consent   ATTRIBUTE MANAGEMENT                                | Ρ | D |
| <u>IP-2(2)</u> | Consent   JUST-IN-TIME NOTICE OF CONSENT                      | Р | D |
| <u>IP-3</u>    | Redress   | Ρ | s |
| <u>IP-3(1)</u> | Redress   NOTICE OF CORRECTION OR AMENDMENT                   | Р | S |
| <u>IP-3(2)</u> | Redress   APPEAL  | Р | S |
| <u>IP-4</u>    | Privacy Notice  |   | S |
| <u>IP-4(1)</u> | Privacy Notice   JUST-IN-TIME NOTICE OF PRIVACY AUTHORIZATION | Р | D |
|                |   |   |   |

#### <u>Ownership</u>

Privacy Program (P) or Joint (J)

#### Selection Criteria

Required (R): based on legal, regulatory or policy regs Situationally Required (S): laws and regs that only apply in specific circumstances Discretionary (D): optional based on privacy risk



#### Privacy Authorization Covers Framework for Comprehensive Privacy Management





### **NIST Privacy Framework**





### What to do Now

- Address Privacy and Supply Chain Risks
  - Create or update policy, procedures, etc.
  - Conduct training on NIST guidelines
  - Collaborate to identify and select privacy controls
- Update System Security Plans and other related documentation
- Review and integrate RMF rev 2, Step 0 tasks
  - New systems: Initiation
  - Legacy systems: Operations/maintenance
- Continue to integrate the frameworks across the enterprise



Glenn Keaveny Director D: 703-562-5946 E Glenn.Keaveny@us.gt.com





## References

- <u>https://www.nist.gov/cyberframework</u>
- <u>https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final</u>
- <u>https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final</u>
- <u>https://www.fedramp.gov/</u>
- <u>https://www.nist.gov/privacy-framework</u>
- <u>https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final</u>
- <u>https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final</u>

