You Had Me at ‘Compliance’:  
Get ready for your close-up with Federal regulations

500 Federal Street  
Suite 540  
Troy, NY 12180  
www.greycastlesecurity.com  
(800) 403-8350

PRESENTER

Stephen Lau  
Senior Security Specialist  
GreyCastle Security  
slau@greycastlesecurity.com
GOAL ONE
Understand the difference between security and compliance.

GOAL TWO
Awareness of the complex Federal regulatory environment.

GOAL THREE
Awareness of standards and paths forward.

SECURITY AND COMPLIANCE

IS THERE A DIFFERENCE?
SECURITY AND COMPLIANCE

IS THERE A DIFFERENCE?

COMPLIANCE DOES NOT EQUAL SECURITY.

• You can be compliant and have insecure systems
• You can have secure systems and be non-compliant

SECURITY AND COMPLIANCE: FINDING A BALANCE

• Identify organization’s risk appetite
  • Ongoing conversation between stakeholders and leadership

• Some factors that influence risk appetite
  • Organizational structure
  • Strong governance or decentralized?
  • Available resources
  • Maturity of organization’s security program
  • External / internal expectations
  • What is everyone else doing?
  • What is considered best practice?
• Nature of the risk
TERMS & DEFINITIONS

- **Information Security / Cybersecurity** – Used interchangeably in Federal landscape. Most Federal regulations use cybersecurity

- **Control** – Measures that modify risk (NIST SP 800-53)
  - Examples include policy, anti-virus, and physical locks

- **Compensating control** – Equivalent or comparable protection for an information system. (NIST SP 800-53)

- **Nonconformity** – Misalignment between regulation or standard and practice or documentation

- **Corrective action / Plan of action and milestones (POA&M)** – Activity to address a nonconformity

FEDERAL REGULATORY LANDSCAPE

- Regulations lag behind technology
  - Often focused on threat du jour (d’hier)

- Can be contradictory or vague
  - Often created by non-technologists

- Complex
  - Approximately 900 NIST SP 800-53 controls

- Moving toward a risk-based approach
  - Increases flexibility for security
  - Increases complexity for compliance
  - Less checkbox security / More “explain why”
(SOME) FEDERAL STANDARDS AND REGULATIONS

• Federal Information Management Security Management Act / Federal Information Processing Standards (FISMA / FIPS)

• National Institute of Standards and Technology (NIST) Risk Management Framework

• NIST Cybersecurity Framework
  • Uses risk management to address cybersecurity

• Federal Risk and Authorization Management Program (FedRAMP)
  • Addresses cybersecurity for cloud services

FISMA / FIPS

• Developed in 2002 (reformed in 2014) by Federal government
  • Often used and abused

• Applicable to:
  • Federal systems
  • State agencies administering Federal programs
  • Private companies with Federal contracts

• Related documents.
  • FIPS 199 – System categorization - High / Medium / Low
  • FIPS 200 – Minimum security requirements
  • NIST SP 800-53 Revision 4 – Catalog of security controls
NIST SPECIAL PUBLICATION 800-53 Rev 4

- Catalog of security controls broken up into 18 control families
  - 3 Baselines (Low / Medium / High)
  - Each control family has control enhancements

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Family</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Access Control</td>
<td>Technical</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training</td>
<td>Operational</td>
</tr>
<tr>
<td>AU</td>
<td>Audit and Accountability</td>
<td>Technical</td>
</tr>
<tr>
<td>CA</td>
<td>Security Assessment and Authorization</td>
<td>Management</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
<td>Operational</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning</td>
<td>Operational</td>
</tr>
<tr>
<td>IA</td>
<td>Identification and Authentication</td>
<td>Technical</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
<td>Operational</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance</td>
<td>Operational</td>
</tr>
<tr>
<td>MP</td>
<td>Media Protection</td>
<td>Operational</td>
</tr>
<tr>
<td>PE</td>
<td>Physical and Environmental Protection</td>
<td>Operational</td>
</tr>
<tr>
<td>PL</td>
<td>Planning</td>
<td>Management</td>
</tr>
<tr>
<td>PS</td>
<td>Personnel Security</td>
<td>Operational</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
<td>Management</td>
</tr>
<tr>
<td>SA</td>
<td>System and Service Acquisition</td>
<td>Management</td>
</tr>
<tr>
<td>SC</td>
<td>System and Communication Protection</td>
<td>Technical</td>
</tr>
<tr>
<td>SI</td>
<td>System and Information Integrity</td>
<td>Operational</td>
</tr>
<tr>
<td>PM</td>
<td>Program Management</td>
<td>Management</td>
</tr>
</tbody>
</table>

NIST RISK MANAGEMENT FRAMEWORK
METHODS TO ADDRESS RISK

• Avoid
  • Don’t do whatever it is that causes the risk

• Mitigate
  • Implement a control to modify / reduce the risk

• Transfer
  • Transfer the risk to a third party
  • Examples: Obtain insurance or outsource the activity (e.g. cloud)

• Accept
  • When the cost to mitigate the risk outweighs the benefit
  • Often used in risks associated with outdated technology or a low risk probability

*Addressing risk does not necessarily mean eliminating risk!*

NIST CYBERSECURITY FRAMEWORK

• Originally published in 2014
  • Targeted for operators of critical infrastructure

• Effort to further shift towards risk management based cybersecurity

• 5 functions and 22 categories
  • Each category has subcategories or outcomes and controls
  • 98 subcategories
NIST CYBERSECURITY FRAMEWORK

OTHER STANDARDS AND REGULATIONS

• Industry specific standards
  • NERC CIP Cybersecurity Standards

• Internationally accepted standards
  • ISO/IEC 27001:2013
  • Center for Internet Security (CIS) Critical Security Controls

Not an exhaustive list – Your mileage will vary.
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC)

- 2006 - Federal Energy Regulatory Commission (FERC) designated NERC to be the United States Electric Reliability Organization (ERO)
- NERC Critical Infrastructure Protection (CIP)
  - 11 standards with controls.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-002-5.1a</td>
<td>BES Cyber Security Categorization</td>
</tr>
<tr>
<td>CIP-003-6</td>
<td>Security Management Controls</td>
</tr>
<tr>
<td>CIP-004-6</td>
<td>Personnel &amp; Training</td>
</tr>
<tr>
<td>CIP-005-5</td>
<td>Electronic Security Perimeter(s)</td>
</tr>
<tr>
<td>CIP-006-6</td>
<td>Physical Security of BES Cyber Systems</td>
</tr>
<tr>
<td>CIP-007-6</td>
<td>System Security Management</td>
</tr>
<tr>
<td>CIP-008-5</td>
<td>Incident Reporting and Response Planning</td>
</tr>
<tr>
<td>CIP-009-6</td>
<td>Recovery Plans for BES Cyber Systems</td>
</tr>
<tr>
<td>CIP-010-2</td>
<td>Configuration Change Management and Vulnerability Assessments</td>
</tr>
<tr>
<td>CIP-011-2</td>
<td>Information Protection</td>
</tr>
<tr>
<td>CIP-014-2</td>
<td>Physical Security</td>
</tr>
</tbody>
</table>

ISO / IEC 27001 INFORMATION SECURITY MANAGEMENT

- International standard
- Focuses on governance and process vs. specific technologies
  - Information Security Management System (ISMS)
- Attempts to achieve a more wholistic approach to information security
  - Information security and risk decisions at the organizational level
  - Reduces silo effects
- 10 Mandatory Clauses + Annex of 18 controls
CENTER FOR INTERNET SECURITY (CIS) CRITICAL SECURITY CONTROLS

- Originally developed by SANS Institute
  - SANS Top 20 Security Controls
- Focuses on controls
  - Risk is based upon historical incidents and situations analyzed by CIS and SANS
- Controls are least common denominator

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 1</td>
<td>Inventory of authorized and unauthorized devices</td>
</tr>
<tr>
<td>CSC 2</td>
<td>Inventory of authorized and unauthorized software</td>
</tr>
<tr>
<td>CSC 3</td>
<td>Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers</td>
</tr>
<tr>
<td>CSC 4</td>
<td>Continuous vulnerability assessment and remediation</td>
</tr>
<tr>
<td>CSC 5</td>
<td>Controlled use of administrative privileges</td>
</tr>
<tr>
<td>CSC 6</td>
<td>Maintenance, monitoring, and analysis of audit logs</td>
</tr>
<tr>
<td>CSC 7</td>
<td>Email and web browser protections</td>
</tr>
<tr>
<td>CSC 8</td>
<td>Malware defenses</td>
</tr>
<tr>
<td>CSC 9</td>
<td>Limitation and control of network ports, protocols, and services</td>
</tr>
<tr>
<td>CSC 10</td>
<td>Data recovery capability</td>
</tr>
<tr>
<td>CSC 11</td>
<td>Secure configurations for network devices such as firewalls, routers, and switches</td>
</tr>
<tr>
<td>CSC 12</td>
<td>Boundary defense</td>
</tr>
<tr>
<td>CSC 13</td>
<td>Data protection</td>
</tr>
<tr>
<td>CSC 14</td>
<td>Controlled access based on the need to know</td>
</tr>
<tr>
<td>CSC 15</td>
<td>Wireless access control</td>
</tr>
<tr>
<td>CSC 16</td>
<td>Account monitoring and control</td>
</tr>
<tr>
<td>CSC 17</td>
<td>Security skills assessment and appropriate training to fill gaps</td>
</tr>
<tr>
<td>CSC 18</td>
<td>Application software security</td>
</tr>
<tr>
<td>CSC 19</td>
<td>Incident response and management</td>
</tr>
<tr>
<td>CSC 20</td>
<td>Penetration tests and red team exercises</td>
</tr>
</tbody>
</table>
WHERE TO FROM HERE?

• Most of standards overlap each other
  • You may be required to comply with one or more standards
  • Pick a path and justify it
  • Identify mappings

• Develop a risk based approach to information security and compliance

• Compliance becomes more difficult to identify and document

RISK BASED SECURITY AND COMPLIANCE

• Less focus on the technology (how)
• Address the actual risks and threats
  • Minimize paper tiger threats
• Risk decisions made at the organizational level
  • Can be difficult with decentralized organizations
• Address risk with controls
  • Avoid / mitigate / transfer / accept
RISK BASED APPROACH TO COMPLIANCE

• Perform and document an annual quantitative risk / gap assessment.
  • Those doing should not be the ones assessing
  • More conversational / less check-boxing

• Identify risks that fall above your organization’s risk acceptance criterion
  • Your organization’s risk acceptance criterion may initially be high

• Risks that fall above your risk acceptance criterion should be Corrective Actions / POA&Ms

COMPENSATING CONTROLS

• Equivalent or comparable protection for an information system. (NIST SP 800-53)

• Most standards have flexibility in “how”
  • Use this flexibility along with risk management to address gaps

• Document and gain approval of rationale
  • Did I mention document?

• Example compensating control:
  • Encryption of databases – can be expensive and operationally problematic
  • Compensating controls: Extensive logging of access, tighter access requirements, data loss prevention monitoring
CORRECTIVE ACTIONS / POA&Ms

- Track and document Corrective Actions
- Identify and assign an owner / champion
  - Hold these individuals responsible
- Identify risk treatments (avoid / mitigate / transfer / accept)
- Identify and document any compensating controls
- Assign a timeline for implementation
- Document progress of implementations and resolution (if any)
- If nothing is done, you’ve effectively operationally accepted the risk, at least for now

Be realistic!

SECURITY AND COMPLIANCE ARE NOT THE SAME THING

IMPLEMENT A RISK BASED APPROACH TO SECURITY AND COMPLIANCE

BE PROACTIVE AND REALISTIC
QUESTIONS?

slau@greycastlesecurity.com
(800) 403-8350
www.greycastlesecurity.com