Federal Computer Security Managers’ Forum

US Census Bureau
Risk Management Framework

August 27, 2015

Jaime Lynn Noble
Agenda

- Defining Characteristics of Census Bureau’s RMF Program
  - Focus on Risk
  - Integration of IT Security Functions
  - Stakeholder-Focused Implementation
- How We Did It – Risk Reporting and Continuous Monitoring
- RMF Program Accomplishments
- RMF Program Scalability and Future State
Characteristics of Census Bureau’s RMF Program

The Census Bureau implemented the RMF Program in accordance with NIST SP 800-37 Revision 1, With three differentiated characteristics.

- **Focus on Risk as Driving Factor**
  - Treat risk as center of equation

- **Integration of IT Security Functions**
  - Break down functional silos to achieve program efficiencies

- **Stakeholder-focused implementation**
  - Place emphasis on stakeholders/end-users
Our Differentiators - Focus on Risk

Risk to the enterprise serves as the core element of our decision making process for cyber actions. Focusing on risk, rather that compliance, allows the bureau to make business-oriented decisions.

<table>
<thead>
<tr>
<th>Application of security controls</th>
<th>Risk Profile Questionnaire to scope and tailor controls based on business and technological factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development of risk metrics</td>
<td>Established risk “points” for each control based on potential impact to Confidentiality, Integrity, and Availability and set an agency risk threshold</td>
</tr>
<tr>
<td>Increased use of Common Controls and Overlays</td>
<td>Established 3 tiers of Common Control Providers (CCP): Technology-based, Organizational, and Enterprise covering 80% of baseline security controls</td>
</tr>
</tbody>
</table>
Incorporate security engineering recommendations in Risk Profile

Embed security engineers in Integrated Project Teams to facilitate security early in the development lifecycle

Incorporate results from automated scanning and manual security control assessments into single risk report

Correlating previously siloed functions allowed the Bureau to realize cost and process efficiencies in execution across workstreams.
Our Differentiators - Stakeholder-Focused Implementation

Security **stakeholders** and **senior management** were actively involved in designing the RMF program to create support for change at all levels

<table>
<thead>
<tr>
<th>RMF Piloting</th>
<th>Governance and Training</th>
<th>Risk Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Interviewed individuals from system-level staff to senior management to garner feedback on proposed RMF implementation</td>
<td>• Developed and executed detailed Change Management strategy</td>
<td>• Generate on-going Risk Reports that include results of ISCM assessments</td>
</tr>
<tr>
<td>• Implemented phased, process pilots with targeted business areas and obtained feedback</td>
<td>• Hold bi-monthly Information Security Community forums</td>
<td>• Detailed assessment results with risk points associated with each control failure</td>
</tr>
<tr>
<td>• Obtained key stakeholder and senior management buy-in</td>
<td>• Hold monthly policy working group meetings</td>
<td>• Risk-based decision-making capabilities (e.g. spending, remediation prioritization)</td>
</tr>
<tr>
<td></td>
<td>• Deliver role-based training</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Deliver content-specific training (e.g. Process, 800-53 Rev 4)</td>
<td></td>
</tr>
</tbody>
</table>
How We Did It - Risk Reporting

Risk reporting on assessment status allows for On-going Authorization of systems and gives our stakeholders the tools to understand and manage cyber risk.

- **Trend in overall residual risk**, broken down by inherited risk, accepted risk, and risk to be mitigated by the POA&M

- **System-specific risk analysis**

- **Top risk contributors by security controls & system component**

- **Status of open POA&Ms**
How We Did It - Information System Continuous Monitoring

ISCM consists of continuous assessments, reporting, and authorization of information systems to monitor security risks.

- **Continuous Assessment**
  - Supports FISMA compliance for ongoing assessment of security control effectiveness.
  - SCAP provides protocol to normalize data from manual and automated assessments.

- **Continuous Authorization**
  - Enables near real-time risk management of information systems.

- **Continuous Reporting**
  - Increases situational risk awareness and supports FISMA reporting requirements.
RMF Program Results

Implementation of the RMF Program at the Census Bureau has yielded numerous **qualitative** and **quantitative results**.

- Risk reports provided to senior management enabled risk-based, mission-aligned decision making.
- Average risk per system reduced from 20% to less than 5%.
- POA&M closure times reduced by up to 75%.
- Cost to apply security controls reduced 90%.
Scalability and Next Steps for Our Program

The RMF Program at the Census Bureau was implemented for scalability, to address current and future cybersecurity needs.

- Incorporation of Federal cyber sprint objectives, including:
  - High-Value Asset determination
  - Enhanced Patch Management Processes
  - Use of Multi-factor Authentication

- Next steps: Increased integration of critical security activities, including:
  - Coordination with Incident Response Management
  - Dynamic re-allocation of control risk points based on threat landscape
  - Correlating risk with cost for efficient cyber resource allocation
Questions?