Continuous Monitoring in a Risk Management Framework

US Census Bureau

Oct 2012

Agenda

- Drivers for Continuous Monitoring
- What is Continuous Monitoring
- Continuous Monitoring in a Risk Management Framework (RMF)
- RMF Cost Efficiencies
- RMF Lessons Learned

Drivers for Continuous Monitoring

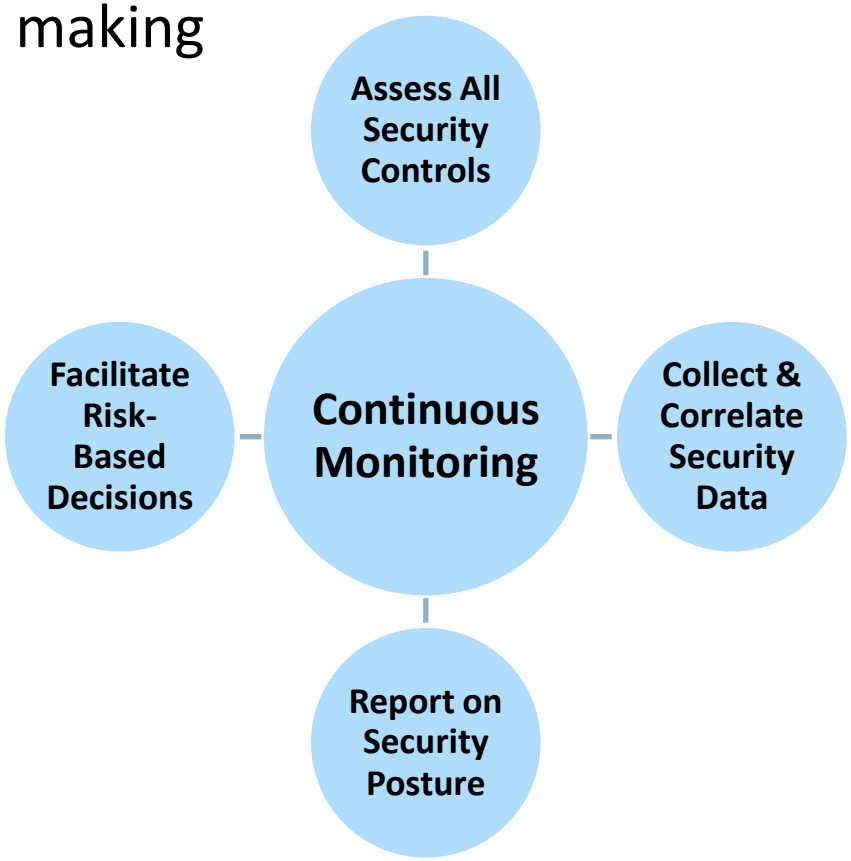
Regulatory change and **increasing demand** are driving the search for a **viable** Continuous Monitoring (CM) **solution**

Regulatory Change	Industry Momentum	Budgetary Concerns
• **OMB A-130** will be updated to **require** Continuous Monitoring • House and Senate **proposed legislation** that mandates Continuous Monitoring	• Departments are planning **transitions** to Continuous Monitoring • DHS/FNS plans to provide **tools and services** for Continuous Monitoring	• Agencies have **budgetary incentives** to take advantage of **cost efficiencies** from Continuous Monitoring • Agencies want to "**end the spend**" on **C&A** activities

What is Continuous Monitoring?

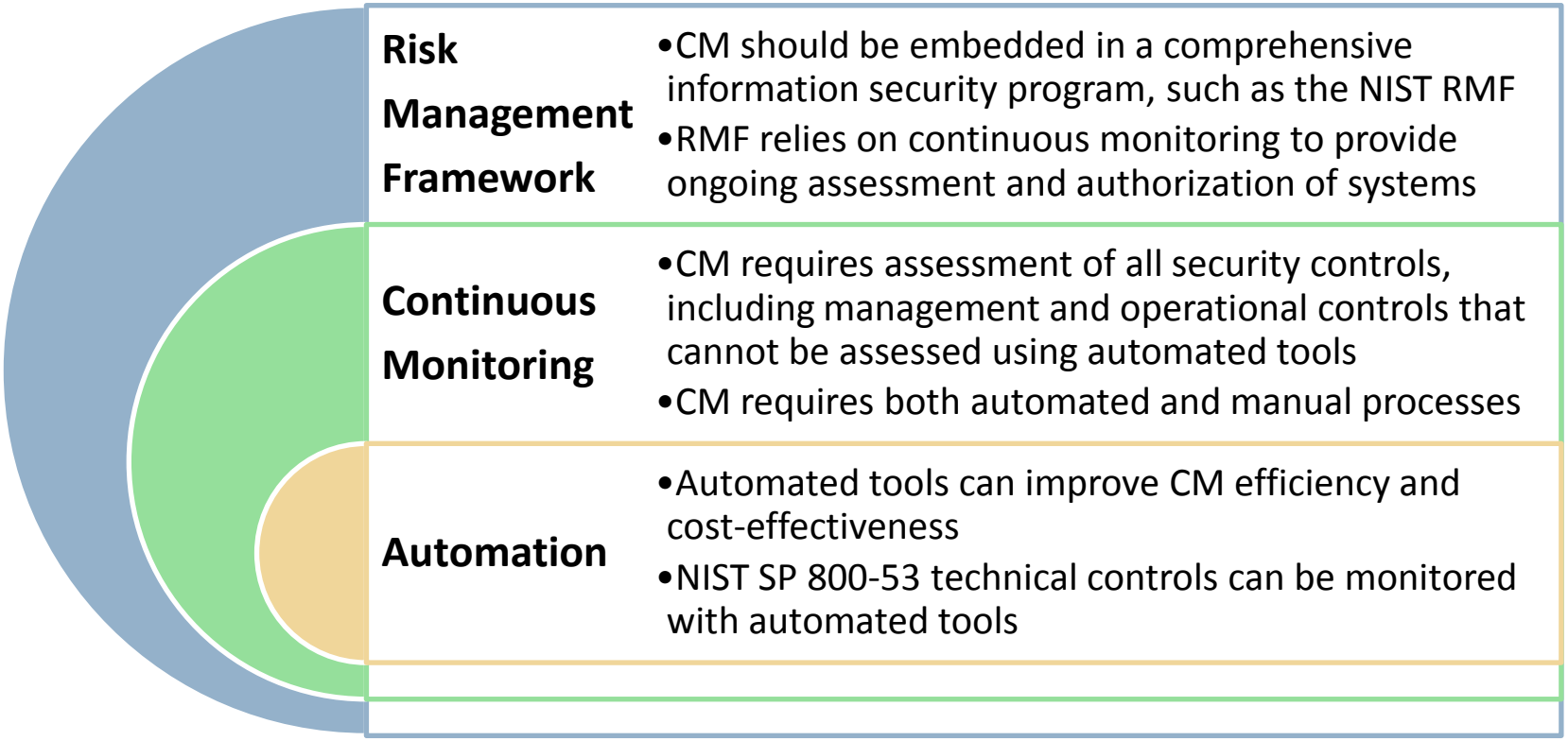
NIST SP 800-137 defines continuous monitoring as **ongoing awareness** of **information security**, vulnerabilities, and threats to facilitate **risk-based** decision making

- CM involves **ongoing assessment** and analysis of the effectiveness of **all security controls**
- CM provides **ongoing reporting** on the **security posture** of information systems
- CM supports **risk management decisions** to help maintain organizational risk tolerance at acceptable levels



What is Continuous Monitoring?(cont'd)

Continuous Monitoring plays a **central role** in the NIST **Risk Management Framework (RMF)**, which provides a structured but dynamic process for near real-time risk management



Census Bureau Challenges

When **developing** our **approach** to Continuous Monitoring, we needed to answer some **fundamental questions**:

1. Can we **satisfy** our **compliance mandates** while still **moving forward** with a **security-centric** Continuous Monitoring plan?
2. How can we **control** the **scope of work** needed to continuously assess the **full catalog** of security controls?
3. How can we drive higher levels of involvement with **our executive stakeholders** to make risk-based decisions?
4. How can we afford to do all of this on our **existing budget**?

What are RMF Benefits?

The RMF **transforms** the traditional Certification & Accreditation (C&A) process into a **risk-based approach** for managing security

RMF

Elimination of 3-Year Certification & Accreditation (C&A) Cycle

Single point-in-time assessments are replaced with Continuous Monitoring

Cohesive Framework for Risk-Centric Decision-Making

Risk Profiles correlate the mission, business, and technology factors that drive IT systems

Increased Use of Automated Security Assessments

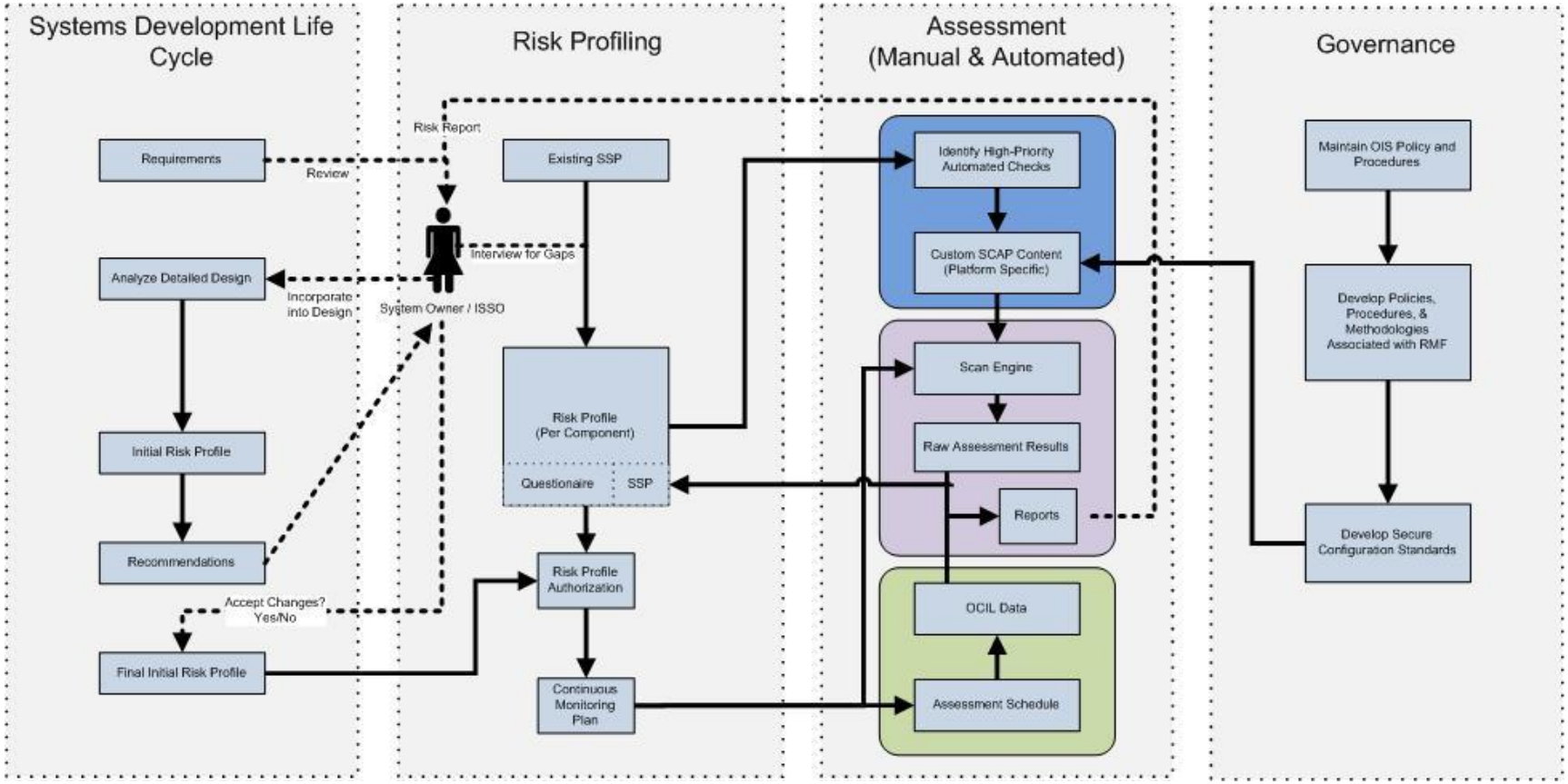
Existing IT toolsets are leveraged to reduce LOE for assessments

Comprehensive reporting on risk and compliance status

Key metrics are incorporated into regular executive reporting

RMF at Census

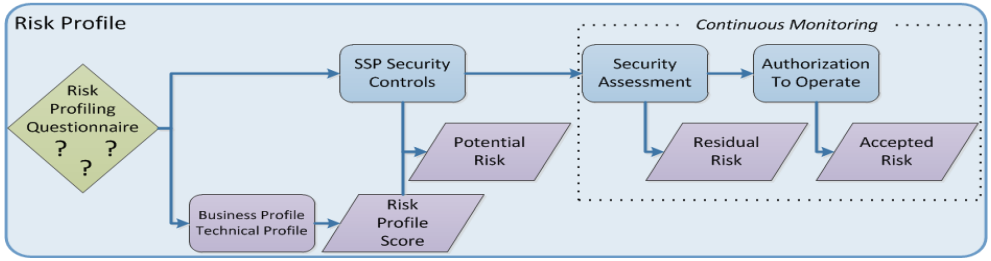
The RMF program at Census consists of **SDLC** integration, **Risk Profiling**, **manual** and **automated Assessments**, and **Governance**



RMF at Census – Risk Profile

The **Risk Profile** is a key **element** of the Census RMF deployment

- **Continuous Monitoring** of **all** security controls can be time and resource **prohibitive**

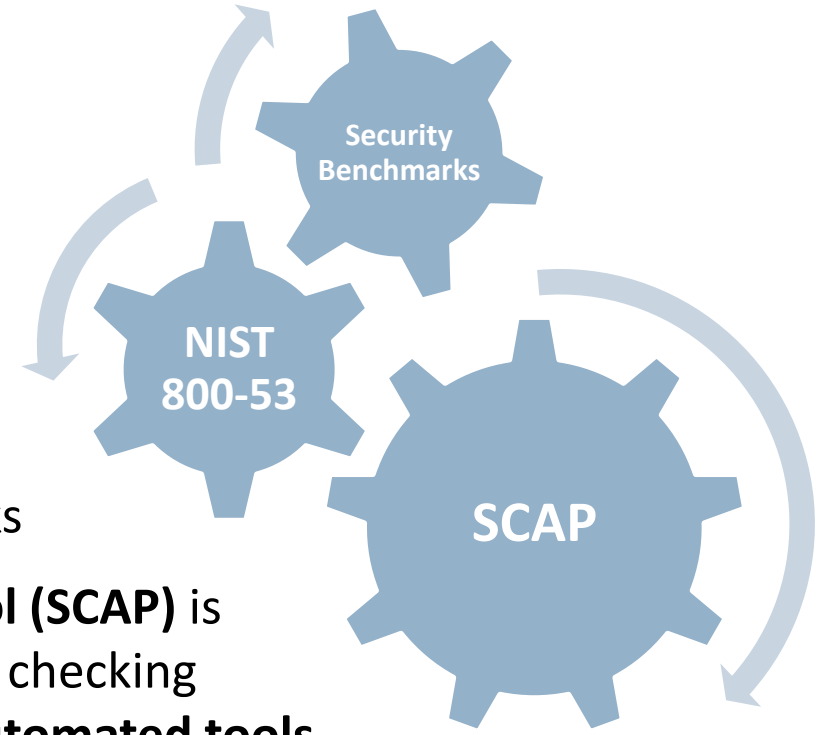


- The **Risk Profile** makes it possible to perform Continuous Monitoring of all implemented security controls by using a **risk-based approach** to **prioritize** control assessments
- **Business** and **technical factors** are considered to identify a component's Risk Profile, which determines the **assessment frequency** for each control based on its associated risk
- The **Risk Profile** leverages **Enterprise Common Control Providers (ECCPs)** to reduce the number of security controls to be assessed, **reducing** the **scope of work** while **maintaining compliance**

RMF at Census – Automation

Security automation is a **critical enabler** of the Census RMF deployment by helping to **reduce costs**, **increase efficiency**, and **improve** the **reliability** of Continuous Monitoring efforts

- **Security configuration benchmarks** form the basis for the automation requirements
- **Automated compliance checks** are created, customized, and **mapped to NIST SP 800-53** technical controls. Automated controls assessments are conducted using the automated checks
- **Security Content Automation Protocol (SCAP)** is used to provide a **standard format** for checking security configuration settings with **automated tools**

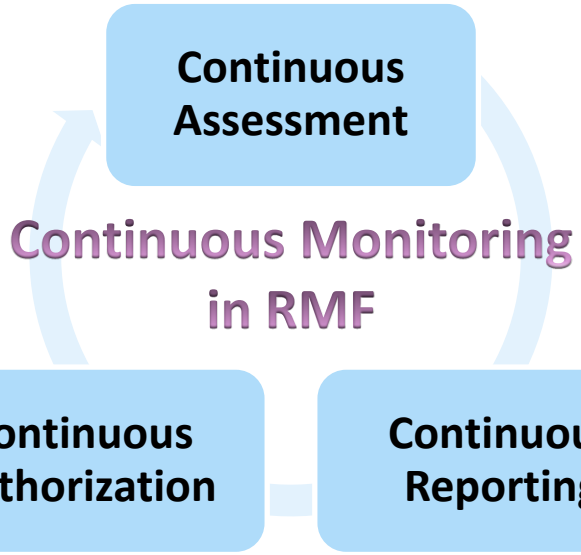


Continuous Monitoring in RMF

Continuous Monitoring in a **Risk Management Framework** consists of **continuous** assessments, reporting, and authorization of information systems to **monitor security risks**

Supports **FISMA compliance** for ongoing assessment of security control effectiveness

SCAP provides a unifying protocol to **normalize data feeds** from both automated and manual assessments



Enables near real-time **risk management** of information systems

Increases situational **risk awareness** and supports **FISMA reporting** requirements

Continuous Assessment

A system is continuously assessed according to the **assessment frequency** determined by its **Risk Profile**

- Security controls with **higher risk** are **assessed more frequently** than controls associated with lower risk
- More reliance on **automated assessments** support a higher frequency of assessments with minimal manual effort
- System stakeholders provide assessors with **access to documentation** so assessors can independently gather evidence for controls

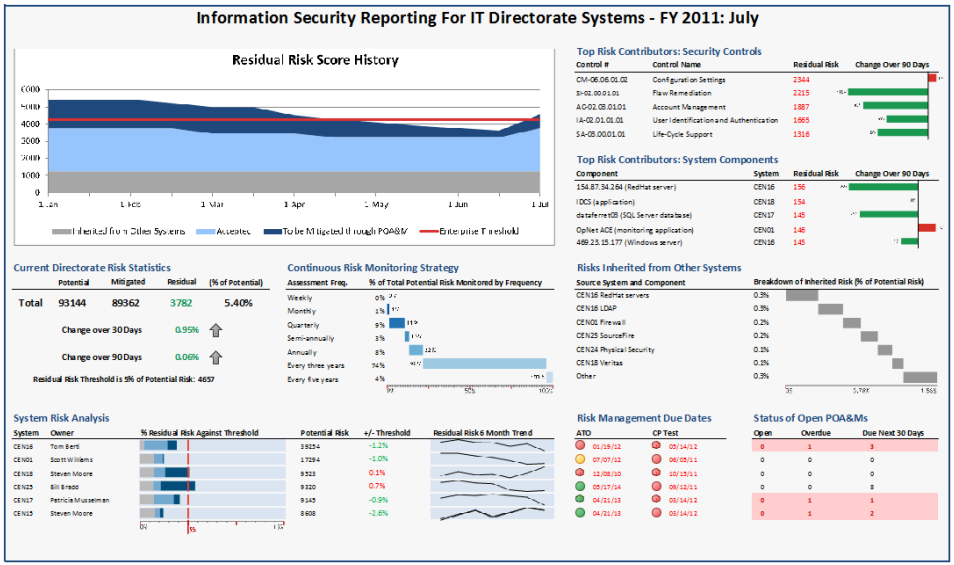
Security assessment process will be **streamlined** to **reduce** the **Level of Effort** (LOE) for system stakeholders

- **Assessment results** are incorporated back into the system's **Risk Profile** and **reported to stakeholders** based on system ownership and responsibility

Continuous Reporting

Regular risk reporting on assessment status allows for **Continuous Monitoring** of systems. **Authorizing Officials** receive information security reports for **systems** in their CENs:

- **Trend in overall residual risk**, broken down by inherited risk, accepted risk, and risk to be mitigated by POA&Ms
- **System-specific risk analysis**
- **Top risk contributors** by security controls and system components
- **Status of open POA&Ms**



Continuous Authorization

Once a Risk Profile SSP is assessed, the **Authorizing Official** (AO) determines whether the system can **maintain** its **Authorization To Operate** (ATO) and remain in **Continuous Monitoring**

- **System Owner (SO)** reviews the Risk Profile SSP assessment reports to determine which **residual risks to mitigate**
  - **Risk-based approach** means that resources will be allocated towards mitigating risks considered to be most critical
- **AO** reviews the **security authorization package** to determine whether risks are at an acceptable level to maintain an **ATO**
- With an ATO, the information system is **monitored continuously**. The AO can continue to provide **continuous authorization** if the system maintains an acceptable risk posture, as reflected in continuous monitoring reports

Continuous Monitoring Status at Census

Census is taking a **phased approach** to **deploying** Continuous Monitoring in a RMF solution, and is nearing 50% completion

	RMF Strategy & Transition Planning	Continuous Monitoring Design & Pilot	Continuous Monitoring Implementation
Timeline	▪ 3 - 4 months	▪ 8 - 9 months	▪ 3 years
Objective	▪ Understand how the RMF can be tailored to the unique characteristics of Census ▪ Obtain key stakeholder support and strategic direction to set the stage for success down the road	▪ Develop a comprehensive framework of automation and process redesign to implement a continuous monitoring program in lieu of traditional C&A activities ▪ Conduct a pilot to test the program design concepts	▪ Transform existing SSPs to new Risk Profiles – 50% ▪ Utilize tools to develop automated compliance checks – 30% ▪ Develop risk reporting database – 30% ▪ Establish governance processes and change management – 60%

RMF Cost Efficiencies

In response to the **Federal mandate** for Continuous Monitoring, the Census Bureau RMF provides a **cost effective** approach for near real-time **risk management**

RMF Strategy	Cost Savings
✔ **Security Program Consolidation**	**Reduction in cost from replacing duplicative programs** for compliance and vulnerability management with a single, comprehensive **Risk Management Program**
✔ **Leverage of ECCPs**	**80% reduction in the number of controls to be assessed** by leveraging Enterprise Common Control Providers (ECCPs), resulting in lower assessment costs
✔ **Automated Assessments**	**80% reduction in LOE to assess controls** using automated checks instead of manual checks. Five months to recover the cost for automating assessment checks
✔ **POA&M Assistance**	**Reduction in time to open and close POA&Ms**, as remediation steps in the Risk Profile SSP make it easier for ISSOs to develop the remediation strategy for POA&Ms

RMF Lessons Learned

The **transition** to **Continuous Monitoring** in a Risk Management Framework can be facilitated by proper planning for **key considerations**

Transition Planning	Develop a RMF transition strategy tailored to the agency environment
Governance	Establish policies and procedures to support new RMF processes
Change Management	Deploy training and communications to promote new RMF processes
Automation Tools	Capitalize on existing tools to reduce the cost for automating assessments

Questions?

Census Contacts

Tim Ruland
Chief Information Security Officer
US Census Bureau
301.763.2869
Timothy.P.Ruland@census.gov

Jaime Lynn Noble
Risk Management Program Manager
US Census Bureau
301.763.5916
Jaime.L.Noble@census.gov