

Cyber Security and Maintaining Public Trust

Kevin Smith
Chief Information Officer

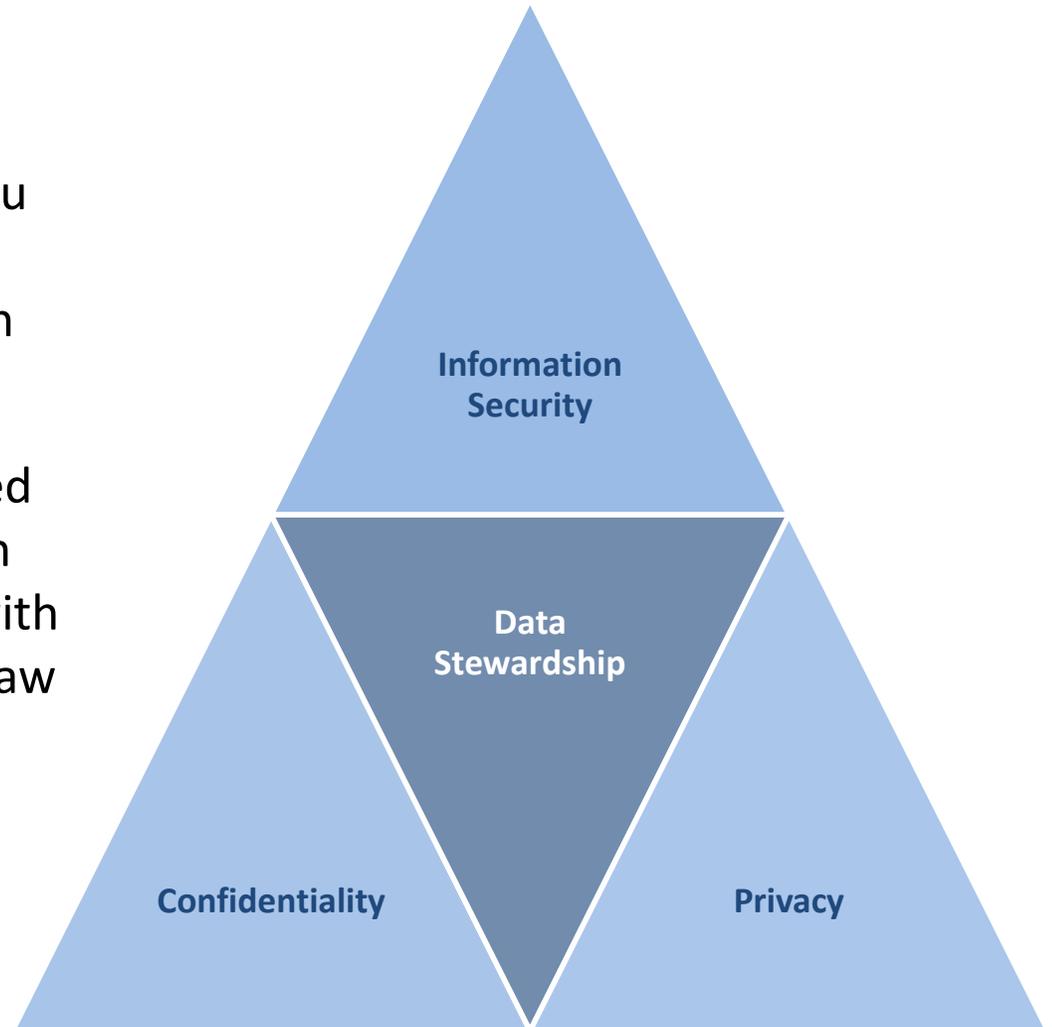


Census Data Stewardship

Our Culture Values Data Security

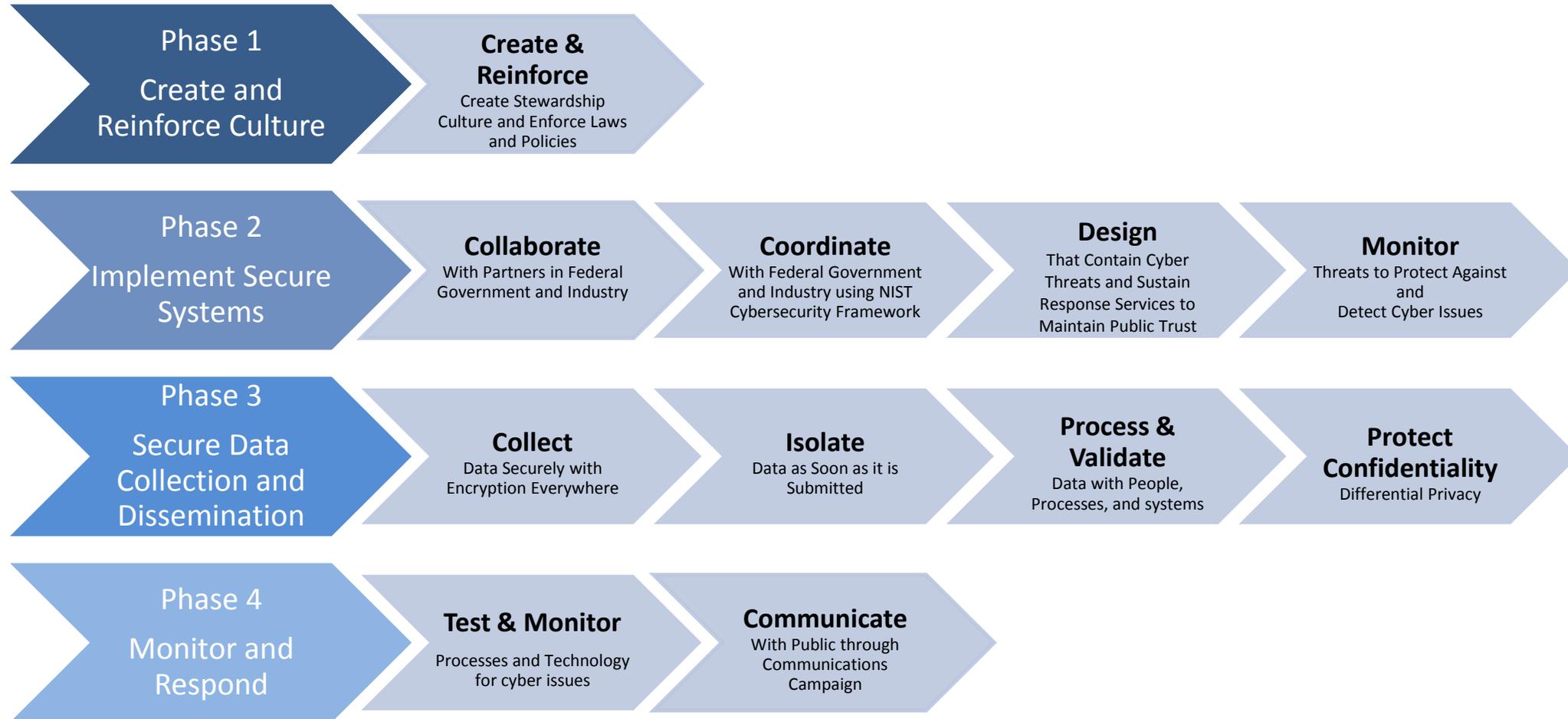
Data Stewardship is the formal process the Census Bureau uses to care for respondent information — from the beginning, when a respondent answers, to the end, when the statistical data products are released.

Data Stewardship is a comprehensive framework designed to protect information over the course of the information lifecycle, from collection to dissemination, and it starts with creating a culture of confidentiality that is based on the law and designed to maintain public trust.



Census Data Stewardship

Our Overall Approach to Maintain Public Trust



2020 Census Cyber Security

Our Cyber Security Approach

Cybersecurity program focus areas:

- Improving **public perception and trust**.
- Proactively addressing **cyber threats** through **design** and **approach**
- Respond immediately to contain threats
- Partnerships to understand and manage threats
 - Federal intelligence community
 - Private industry

**sharing detailed solutions, systems, processes*



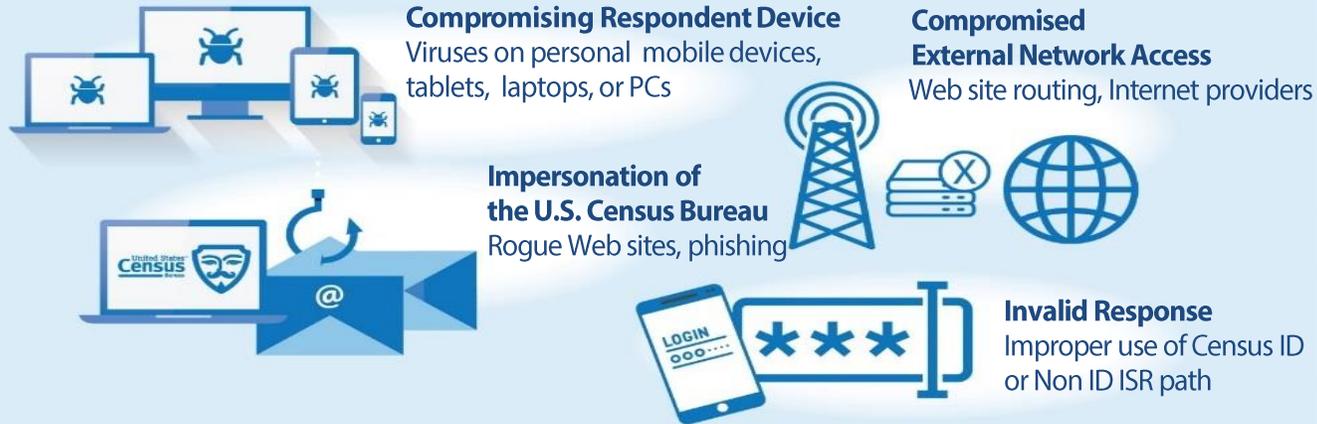
Cyber Threat Landscape

Continuously Evolving

Cyber Threats



External Threats
Beyond
U.S. Census Bureau
Control



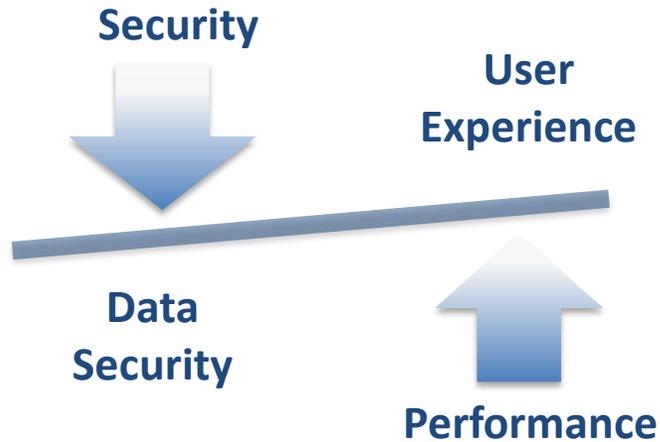
Internal Threats
Within
U.S. Census Bureau
Control



- **External** - Rely on industry and other federal agencies to provide services to resolve threats
- **Internal** - Monitor and directly respond to internal threats to Census Bureau systems through design and approach

Secure System Design

Designed to Contain, Sustain, and Maintain Public Trust



Census design is focused 1st on data security to protect respondents' data and 2nd on user experience so that respondents may confidently respond to the 2020 Census

Contain Issues + Sustain Services = Maintain Public Trust

Employ “Physical Security” Techniques

- “Layer” physical entry with the appropriate level of security (doors, walls)
- “Isolate” separate areas within layers to efficiently handle interactions (lines, guards)
- Lock down valuables behind closed doors (vaults, safes)

External Cyber Threat Mitigation

Relying on Partnerships



External Threat Mitigation Strategies	
Compromising Respondent Device	<ul style="list-style-type: none"> Minimal storing of data on device Encryption of data in-transit for website communications Proactive public outreach and awareness campaign
Compromised External Network Access	<ul style="list-style-type: none"> Proactive monitoring of site performance and activity Proactive monitoring for unauthorized or unusual connection attempts Industry and interagency coordination and information sharing
Impersonation of U.S. Census	<ul style="list-style-type: none"> Proactive identification of rogue websites Interagency coordination and information sharing Proactive public outreach and awareness campaign
Invalid Response	<ul style="list-style-type: none"> Automated analysis of individual responses to identify irregularities Analysis of identified irregularities Data flow analysis

Internal Cyber Threat Mitigation

Monitoring and Directly Responding



Internal Threats
Within
U.S. Census Bureau
Control

Internal Threat Mitigation Strategies	
Disruption to the Internet Self Response Web Site	<ul style="list-style-type: none"> Monitoring for traffic spikes and unusual activity in systems/applications Proactive identification of malicious traffic and robots Cyber threat intelligence (federal, commercial, state, and local government) Designed to sustain self response services Use of Distributed Denial of Service (DDoS) protection services
Data Breaches	<ul style="list-style-type: none"> Monitoring for irregular data flows Monitoring for unauthorized access Encryption of data in-transit and at-rest System/application penetration testing Security management, monitoring, and analytics Timely patch management Cyber awareness training Proactive public outreach and awareness campaign
Compromised Employee Devices	<ul style="list-style-type: none"> Encryption of data in-transit and at-rest Remote wipe capability Monitoring user activity and detection of malicious end user Two factor authentication Phishing tests

QUESTIONS?