



# Continually Evolving Cybersecurity Program

---

FOR THE 2020 CENSUS

**Kevin Smith**

Associate Director for Information Technology and Chief  
Information Officer

March 29, 2018



# 2020 CENSUS CYBERSECURITY

## Agenda

- Overview
  - Plan
  - Challenge
  - Design
  - Cyber Threat Landscape
  - Approach



# 2020 CENSUS CYBERSECURITY

## Overview

U.S. Census Bureau: Leading source of quality data about the nation's people, places, and economy.

***Cyberattacks impact our data and could compromise our mission:***

- Cybersecurity is our highest IT priority.
- Evolve cybersecurity to meet new threats.
- leveraging best resources and knowledge inside and outside the federal government.





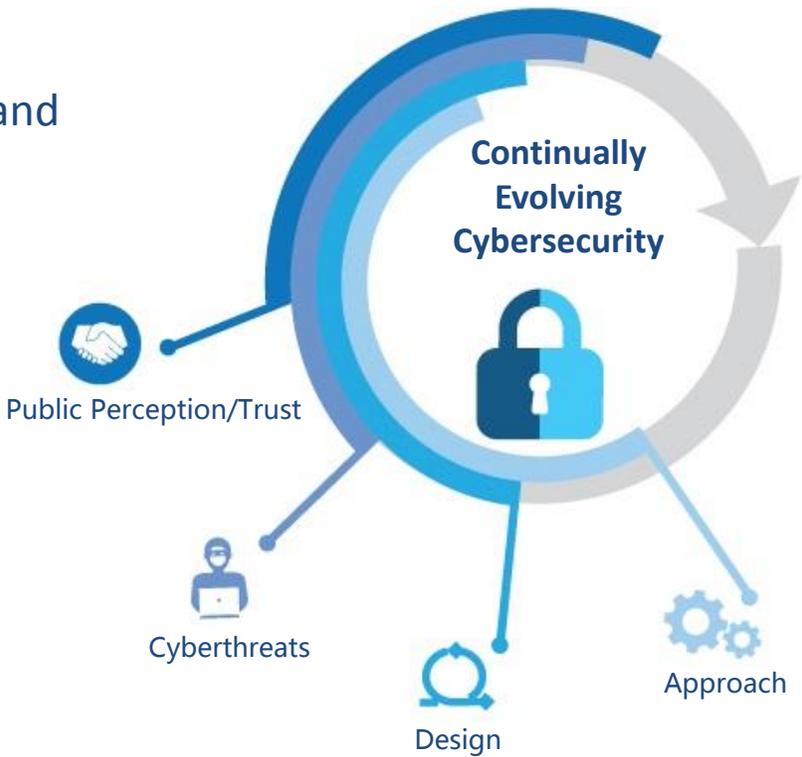
# 2020 CENSUS CYBERSECURITY

## Our Plan

Cybersecurity program focus areas:

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

## Key Components





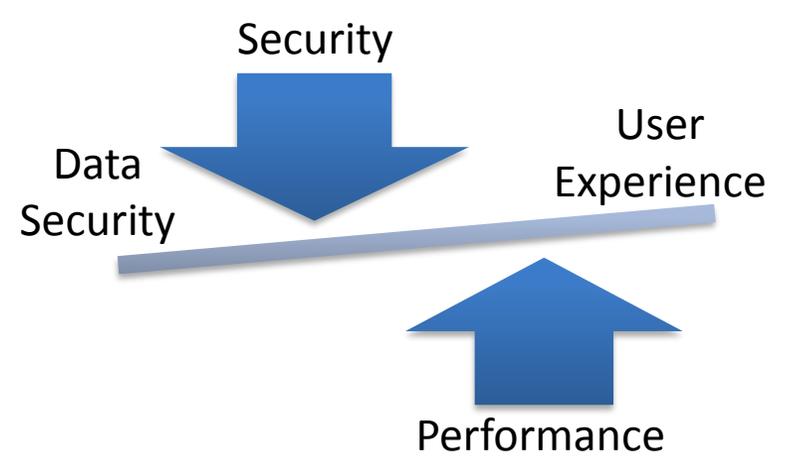
# 2020 CENSUS CYBERSECURITY

## Challenge: Ensure Public Perception/Trust

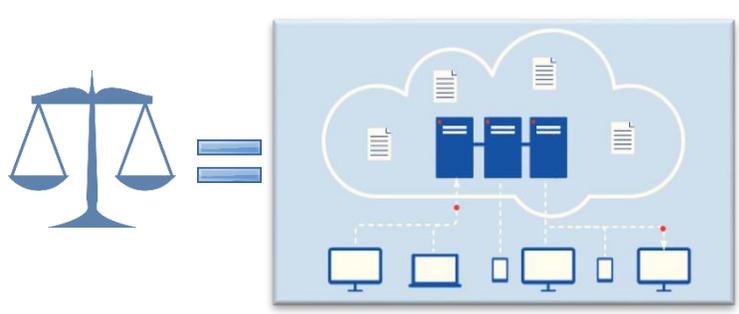
### Top Priorities

- **Data Security** – Protecting respondent data
- **User Experience** – Performance that public expects with confidence that their data will be protected

### Top Priorities are Opposing Forces



### Balance in Cloud Based Solution



### Data Security:

Layer public facing systems in secure segments

### User Experience:

Rapid, Repeatable, and Efficient scaling of isolated segments to ensure performance



# 2020 CENSUS CYBERSECURITY

## Design



Incorporate many layers and levels of isolation.

- Apply right balance of security and performance
- Does not sacrifice overall security.

Create “funnel effect” to minimize undesired users

- Apply very high levels of security early to our publicly facing system.

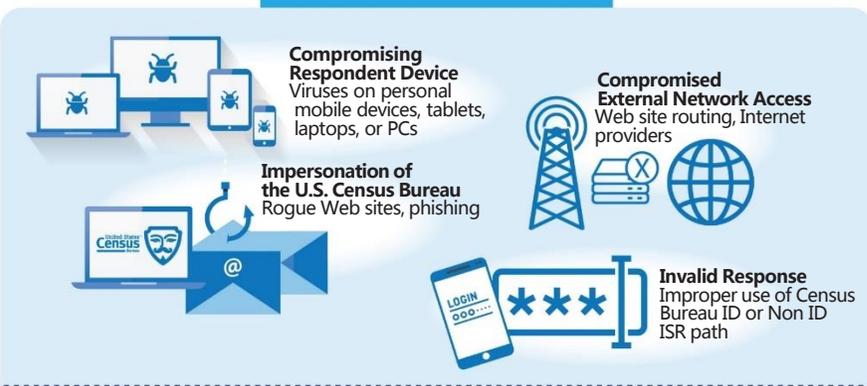


# 2020 CENSUS CYBERSECURITY

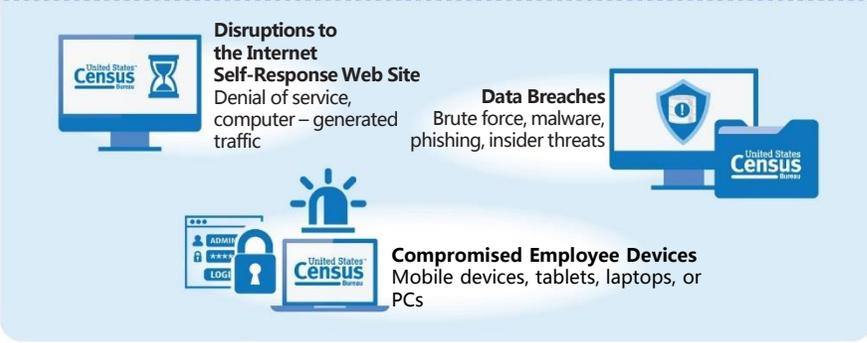
## Cyber Threat Landscape

### Cyberthreats

  
External Threats  
Beyond  
U.S. Census Bureau  
Control



  
Internal Threats  
Within  
U.S. Census Bureau  
Control



A cloud-based system alone does not protect our data from all cyber threats

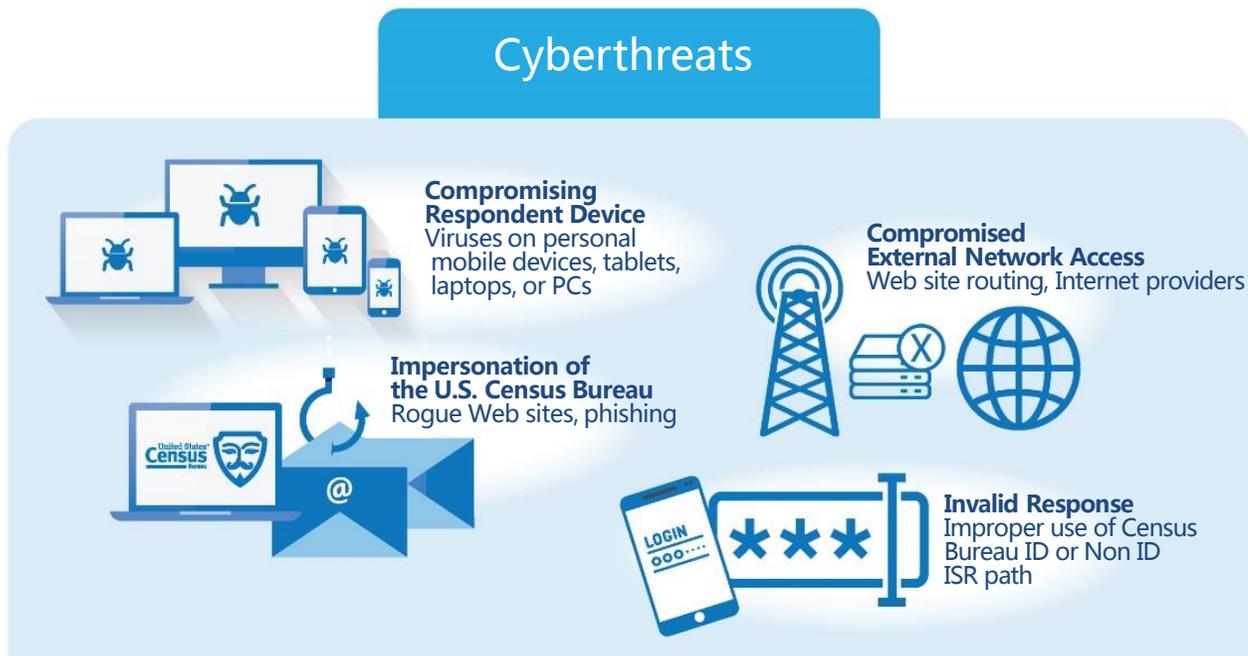
- External - Rely on industry and other federal agencies to provide services to resolve threats
- Internal - Monitor and directly respond to internal threats to Census Bureau systems through design and approach



# 2020 CENSUS CYBERSECURITY

## Cyber Threats: External

- Census Bureau does not have direct control over **external cyber threats**
- We can detect some threats but cannot take direct action to resolve





# 2020 CENSUS CYBERSECURITY

## Cyber Threats: Internal

- Census bureau has the ability to take direct action to prevent and resolve **internal threats**
- Our team proactively monitors known threats

  
**Internal Threats**  
 Within  
 U.S. Census Bureau  
 Control

### Cyberthreats



**Disruptions to the Internet Self-Response Web Site**  
Denial of service, computer – generated traffic

**Data Breaches**  
Brute force, malware, phishing, insider threats

**Compromised Employee Devices**  
Mobile devices, tablets, laptops, or PCs

### Risk Mitigation Strategy



**Federal partners** for unknown threat protection and detection.

**Industry solutions** to assist with known threat protection, detection, and recovery

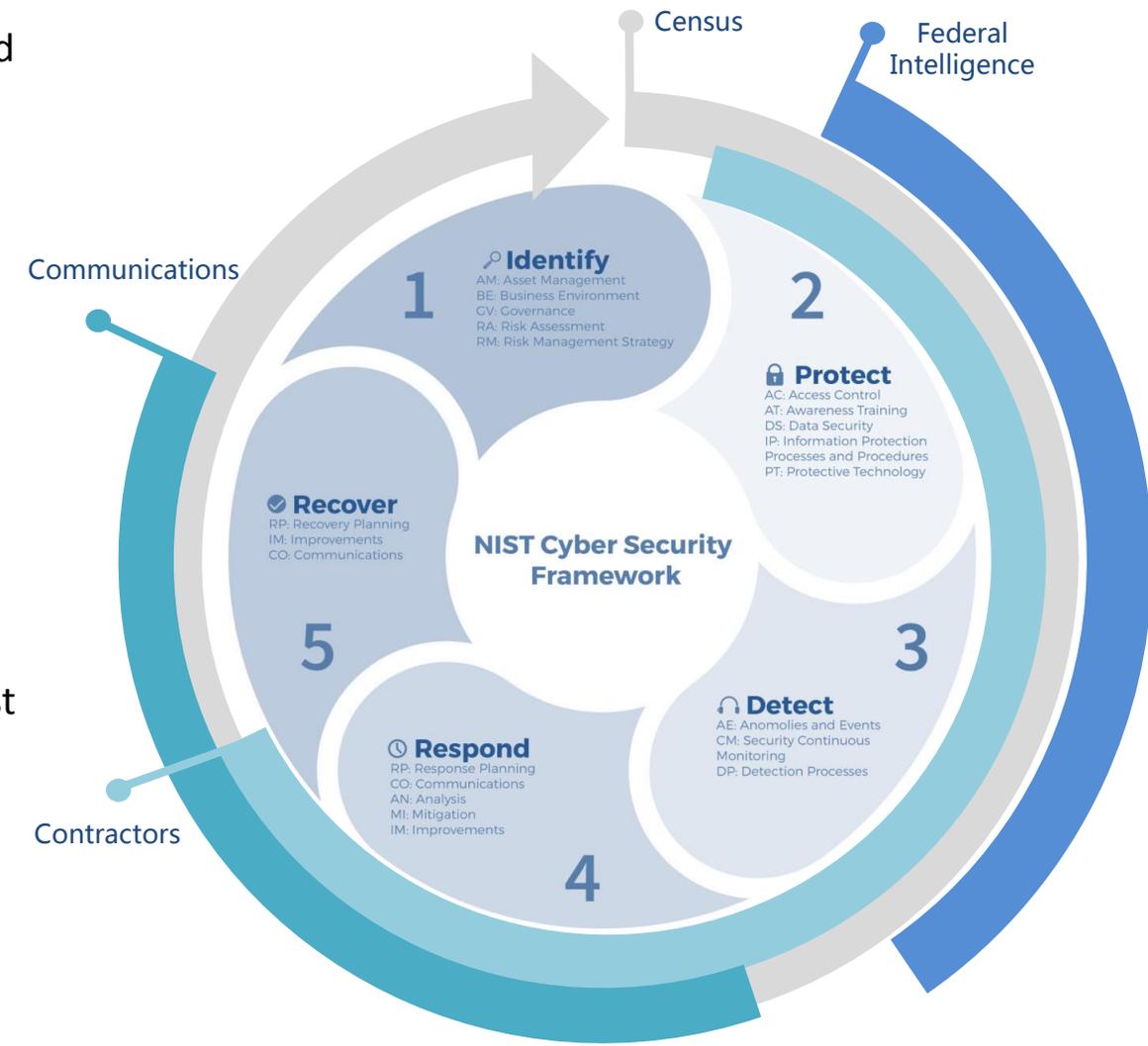
**Our incident response** plan to contain and manage security breaches.



# 2020 CENSUS CYBERSECURITY

## Federal Cybersecurity Framework Responsibilities

- The **Cybersecurity Framework** is the continual lifecycle used to coordinate interactions of people, process, and technology to have a complete approach to Cybersecurity
- **Census** responsible for all areas across Census systems
  - Coherency, Coordination, Consistency
- **Contractors** work within Census to protect, detect, and respond for the systems they maintain.
- **Federal Intelligence Community** can assist in protecting against and detecting cyber threats
- **Communications** coordination necessary ensure public trust and confidence during potential response and recovery





# 2020 CENSUS CYBERSECURITY

## Key Areas and Partners

- **Secure Federal Network Connectivity for 2020 Respondents**

*Working with Industry and Federal Government to ensure scalable and secure federal network connection*

- **Strengthen Incident Response capabilities**

*Advance ability to continually Identify, Protect, Detect, Respond, and Recover from possible cyber threats*

- Improving visibility of cybersecurity issues by implementing tools from private industry and federal government
- Engaging Federal Intelligence Community for a coordinated Federal response.

- **Improve Cybersecurity Posture**

*Improve knowledge, processes, procedures, and/or technology.*

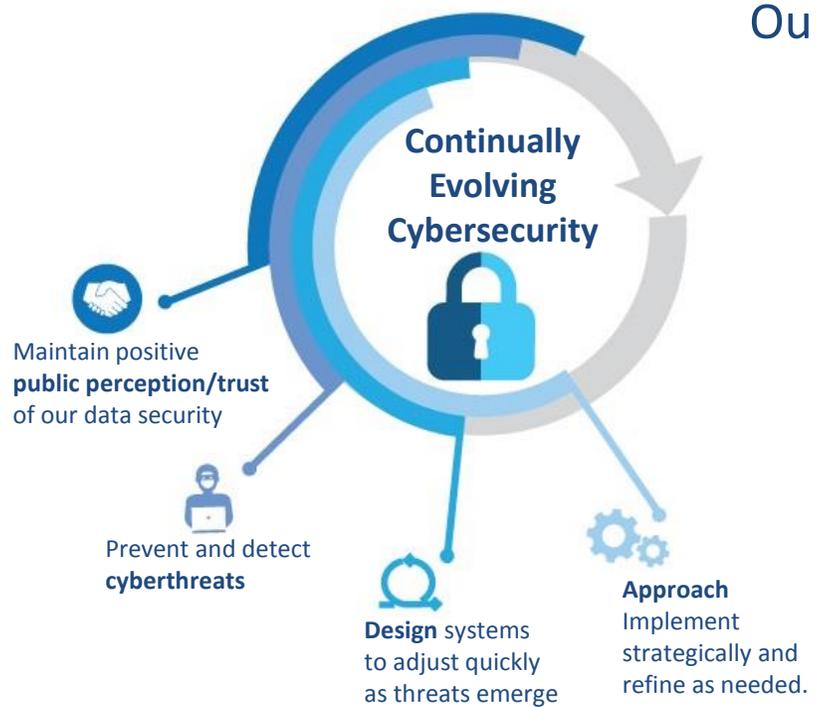
- Improving Knowledge, Processes, and Procedures
  - Regular Cybersecurity briefings with Federal Intelligence Community
  - Test response procedures to cybersecurity incidents through simulations with Federal Partners
- Testing Technology
  - Security Tested Internet Self Response system by Industry and Federal Government
  - Engaging Industry and Federal Government to simulate cybersecurity attacks



# 2020 CENSUS CYBERSECURITY

## Approach

Our approach will **continually be refined** as threats emerge and evolve.



### We Will:

- Maintain the public's trust and confidence by protecting their data and keeping them informed
- Protect, detect, and respond to cyberthreats through technology and partnerships
- Adjust solutions accordingly within our flexible design
- Work with federal and industry partners to help us fill gaps



# 2020 CENSUS CYBERSECURITY

## Summary

External Threats  
Beyond  
U.S. Census Bureau  
Control

Internal Threats  
Within  
U.S. Census Bureau  
Control

### Cyberthreats

- Compromising Respondent Device
- Compromising External Network Access
- Impersonating the Census Bureau
- Inserting Invalid responses
- Disrupting the Internet Self Response Web site
- Data Breach
- Compromised Employee Device

### Data Vulnerabilities

Data on individual devices has minimal value to cybercriminals

Data collected and protected by the Census Bureau

Individual Data + Everyone's Data = High Value

### Risk Mitigation Strategy

Continuous communication and technology mitigate risk

Continually evolving our cybersecurity program to prevent and detect threats

Continually evolving cybersecurity program will give us the best opportunity to:

- ✓ Identify
- ✓ Protect
- ✓ Detect
- ✓ Respond
- ✓ Recover from possible cyber threats

Enable **partners** to get involved in necessary areas.

**Mitigate operational challenges** to adjust quickly as threats are identified to contain for analysis.