From: The JHU Sentinels Cybersecurity Task Force

To: The President of the United States

Subject: Response to Task on Census Bureau Threats and Vulnerabilities

INTRODUCTION

In response to the President's concerns about threat vectors concerning the 2020 Census, our task force performed a cyber risk assessment on the documents provided and our additional research. Based on what we know to date about potential threats in technical structures and data-collection processes, we believe the overall risk to accurate Census data collection is minimal. However, given the importance of the Census and the serious implications of a flawed process, these threats and vulnerabilities must be taken seriously to avoid loss of public confidence in the Census process and results. We discuss our analysis below and provide a recommended course of action to be implemented before Census Day on April 1, 2020.

THREATS AND VULNERABILITIES

We evaluated the potential threats in the documents provided and identified other potential threat vectors and vulnerabilities as described below.

- **Fraud and Impersonation of the Census Bureau.** Bloggers and the *Washington Post* report an email scam where people have been duped into sending in Census-related information in return for a cash rebate. There has been a suggestion that this scam is conducted by nation-state adversaries like the interference in the 2016 election. While the email scam has a significant impact on its victims, we don't believe it constitutes a threat to the Census, and so far, we have seen no evidence of any nation-state involvement.
- **Compromised Survey Devices/Networks.** Several security vulnerabilities were indicated in the Census Bureau infrastructure audit, including resource shortfalls in management of the cloud server integrators as well as lack of testing of field enumeration devices. In addition, several scheduled testing events were cancelled. While these potential threats might make the Census vulnerable to cyberattacks, our analysis suggests the processes used by the Bureau including encryption of data in transit and at rest reduce the overall vulnerabilities. We believe the risk to the validity and integrity of Census data from threats to the infrastructure is manageable.
- **Insufficient Level of Census Staff with Subject-Matter Training.** Another concern raised in the audit is that the Census Bureau staff and their contractors may not be sufficiently trained in cybersecurity. For instance, a cyber attacker may gain access via spear-phishing on bureau or contractor personnel and manipulate or destroy Census data. This would potentially call the Census results into question or invalidate the data. Although targeted cyberattacks towards Census personnel has not been observed, we believe spear-phishing and similar threats are legitimate concerns.
- **Data Breaches.** Data breaches like those described in the Silk Road release and Rabinara report are a potential threat to any activity like the Census that depends on maintaining data integrity during collection and storage. We think the risk of a breach in Census data is low because the Census Bureau has developed and tested a secure process using strong encryption for collected data in transit and stored data. In addition, Census data would not include the type of Personally Identifiable Information (PII), such as passport numbers and medical records mentioned in these reports. We assess the overall threat of a data breach to be low and believe the PII in the Rabinara report came from non-Census sources.
- **Trolling, Falsification, and Invalid Responses.** The Census Bureau audit also identifies cyber-trolling as a continuing concern. More broadly, the falsification or invalid responses to Census questions could also hamper the data collection process, especially with the emphasis on online Census response. Individuals may submit incorrect or invalid responses due to political motivation or privacy concerns. This hasn't been observed yet but is a possibility.

IMPLICATION AND IMPACTS

While cyber threats persist within the upcoming Census, we do not believe any of the above threats directly undermines the validity of the 2020 Census. However, we assess the technical threats and sensationalistic media reports described above are a continuing concern and must be addressed. **We believe their biggest impact is to public confidence in the Census and its results.**

If the public lacks confidence in the Census, mistrust arises in two major areas: first, **the distribution of seats in the House of Representatives;** second, **the distribution of funds to each state through federal agencies**. The repercussions will be long-lasting and will affect everything from healthcare to education to infrastructure projects.

Other implications of current threat vectors include the following:

- IF a substantial segment of the public feels that their **confidentiality and privacy concerns** are not being addressed in the Census process, THEN response rates to the initial Census would be low; trolling and response falsification will be observed. Increased personnel and budget would be required for follow-up data collection using traditional data collection techniques.
- IF cybersecurity incidents on the 2020 Census infrastructure occurs due to identified or even unidentified vulnerabilities, THEN **public confidence would decline** sharply. Additional efforts would be needed to repair damaged systems and restore affected data, as well as to rebuild public confidence towards the Census.
- IF public and private sectors are unable to use Census results in measuring demands, analyzing trends, and predicting future needs due to **the lack of confidence**, THEN their decision-making processes are inhibited, which affects industrial performance and revenue.

Any of these potential impacts would seriously affect the credibility of the Census process and results. However, we believe that possibility of these impacts can be minimized with a strong Government response as described below.

RECOMMENDED COURSE OF ACTION

To maintain confidence in the Census process and results, **we recommend a robust communication campaign and related activities** to be conducted by the President, the Executive Office, the Secretary of Commerce, and other Cabinet officers to reassure Congress and the public that the Census process is sound, and the results will be accurate.

- The **communication campaign** should include all forms of media, including Presidential tweets and use of the bully pulpit, to ensure the American public that the Federal Government has high confidence in the Census process and results. These communications should also include information about efforts by the Departments of Justice and Commerce to identify and stop Census-related scams or cyber-trolling. Publicizing the government's efforts to catch the ringleaders would secure some measure of justice, reassure the public that the government is taking their privacy and confidentiality seriously, and – most importantly – such efforts would deter other potential wrongdoers tempted to exploit the 2020 Census.
- The President should direct the Attorney General to launch **national and state-level investigations into phishing and internet crimes**. These investigations should be widely publicized and explicitly tied to the Federal effort to protect the Census. Enforcement of the law against scammers would also deter potential hackers who seek illicit profits from the 2020 Census process. Encouraging participation in the Census is the major goal of the communications campaign. President should direct the Secretary of Commerce to invest in targeted advertising over the next few weeks to ensure that a broad range of citizens are aware of the Census and how they can participate. The Attorney General could also remind people about the legal requirement to cooperate with the Census authorities – failure to complete Census forms accurately and completely or providing false answers to Census questions is punishable under Title 13, U.S. Code.
- The President should also direct the Secretary of Commerce **to ensure the readiness of Census enumerator devices** from private contractors within the next 7 days and ensure that backup data collection systems will be operationally ready within the next two weeks, in case electronic systems are compromised. Commerce should also work to mitigate technical threats through real-time monitoring, including inspecting irregular traffic spikes and data flows, identifying unauthorized access, and reviewing irregularities in responses continuously.
- To mitigate **potential foreign threats**, the President should direct the Director of National Intelligence to enhance its collection against potential foreign interference with the Census including collaborating with foreign partners to track down any foreign-based scammers.
- In the event that intelligence reveals foreign attempts to compromise the Census, the President should direct the Secretary of Defense to have **USCYBERCOM prepared to take action** as required to thwart any foreign attempts to interfere with the Census, similar to what was done to prevent interference in the 2018 midterm elections.