From: The JHU Sentinels Cybersecurity Task Force
To: The President of the United States
Subject: Continuing threats to the Census Bureau

Based on events revealed over the last 24 hours, we believe that the situation has escalated to NCCIC **Threat Level 3**. Public confidence in the Census is being seriously eroded by misinformation on social media. Chancellor of Germany is furious as a US-based data breach has victimized the son of the German ambassador. We recommend the following actions supported by a communications campaign to restore the public's confidence in the Census.

SITUATION ANALYSIS

1. **Botnet**, a bot campaign likely originating from Russia or Venezuela, is being used to amplify anti-Census narratives. It may reduce participation in 2020 Census, and potentially affects the democratic process.
2. **Grassroots campaign** to **boycott the Census** has gained traction with its focus on data security and minority rights. It reduces public confidence in the Census.
3. **Data breach** containing sensitive PII is likely unrelated to the 2020 Census. Yet, it requires action because of its impact on our relationship with Germany, a NATO ally.

RECOMMENDED COURSE OF ACTION

The **communication campaign** should include various forms of media, including Presidential tweets and use of the bully pulpit, to raise the public's confidence in the Census process and results.
The following steps should be taken to maximize its effectiveness:

1. **Establish a Cyber Unified Coordination Group (UCG)** in accordance with PPD-41 to coordinate federal and private sector activities. **DoJ and the NCIJTF** should lead efforts of federal and state law enforcement, and the **ODNI through CTIIC** should lead intelligence support efforts.
2. **Regarding botnet, the President should:**
    a. Direct the UCG to collaborate with social media companies (e.g., Twitter) to identify and delete Census-related scam accounts.
    b. Direct the DNI to continue efforts on attribution and draft a presidential finding to authorize covert operations against the botnet by the Central Intelligence Agency and USCYBERCOM under Title 50 of the U.S. Code.
    c. Direct the Department of State to issue démarche (i.e., formal statement or request) to the Russian and Venezuelan governments.
3. **Regarding the Pandora data breach, the President should:**
    a. Direct the Attorney General to prioritize Pandora investigation by the Federal Bureau of Investigation and determine whether federal laws have been broken.
    b. Direct the UCG to work with state attorneys general to conduct state-level investigation and enforce state laws on data security (i.e., security breach notification laws).
    c. Direct the Secretary of State to respond to the German Chancellor on the doxing incident.
4. **Regarding use of sensitive PII, the President should:**
    a. Direct the UCG and FBI to investigate the Ritterson Manufacturing's claim that it bought the data in "good faith" and provide legal knowledge in dealing with illegal sensitive data.

b. Direct the UCG to work with the Multi-state ISAC to share information with the private sector about the impact of data breaches with sensitive PII.