



Cyber 9/12 Strategy Challenge

Intelligence Report I

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

Your team will take on the role of experienced policy advisers, part of a hypothetical cybersecurity task-force, preparing to brief the President of the United States. This packet contains fictional information on the background and current situation involving a major cyber incident affecting US systems. The attacks notionally take place in spring 2020. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The President of the United States needs information on the full range of response options available to the US regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the President.

You are to consider as facts the following pages for formulating your response.

You will use the fictional scenario material presented to perform three tasks:

- 1. Written Situation Assessment and Policy Brief:** Write an analytical policy brief that provides a concise assessment of the situation, addresses potential impacts and risks, and discusses the implications of the cyber incident. Describe policy considerations for different potential state and non-state actors and explore the course of action you are recommending in depth. The length of the brief is limited to two single-sided pages in length. It is due no later than **March 19, 2019** at **NOON EST**. Please submit your written brief here: <https://form.jotform.com/90356394457163>
- 2. Oral Policy Brief:** For the first day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action, recommending it to the President.
- 3. Decision Document:** Teams will also be required to submit a “decision document” accompanying their oral presentation at the beginning of the competition round. The “decision

document” will be a maximum of one single-sided page in length, outlining the team’s response options, decision process, and recommendations. The teams should note that the document is not intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you’re briefing.* You are experienced cyber policy professionals briefing the upper echelons of the US government. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: Cybersecurity Task-Force Central Command
Re: Vulnerabilities in Key US Systems
Date: Sunday 15 March 2020 7:53 a.m.

You are top policy advisers, part of a hypothetical cybersecurity task-force, preparing to brief the President on a developing threat to the United States. Based off initial intelligence, the President has indicated that he is concerned about threat vectors concerning the US Census Bureau and (a) supposed data breach(es) affecting unknown parties. There may be other threat vectors that the President is not yet aware of.

Given the unclear nature of the threat, the President requests your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the US government can or should consider to address these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.


As top policy advisers, in formulating your response you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing a **comprehensive policy recommendation** for the task force:

- **Tab 1 – Scam Email**
- **Tab 2 – Internal Census Audit**
- **Tab 3 – Dark Web Sales Posting**
- **Tab 4 – Rabinara Group Cybersecurity Report**
- **Tab 5 – “Loomis on Cyber” Blogpost**
- **Tab 6 – Washington Post Article**

Tab 1 – Scam Email

 **This message could be a scam.** The sender's account may have been compromised and used to send malicious messages. If this message seems suspicious, let us know and then alert the sender as well (in some way other than email). [Learn more](#)
[Report this suspicious message](#) [Ignore, I trust this message](#)



From: US Census Bureau {Mail to: earliaction@census.org}
Sent: 0913, 02-March-2020
To: Jerry Gergich
Subject: Get a \$20 rebate by filling out your census data ahead of time.
LIMITED TIME ONLY

Dear citizen,

As you may be aware, the Census Bureau has been strategizing heavily this year to find ways to more effectively and efficiently gather our national data. The data collected by our agency is used to make critical decisions such as how to apportion seats in the U.S. House of Representatives, where to spend government money to support community services such as roads and schools, and how states and communities allocate funding for projects such as public health and transportation.

As the official start of the census collection period grows near, we wanted to offer citizens the opportunity to answer our questions early online. To incentivize these citizens, the census bureau has decided to offer individuals who fill out their questionnaires online a **\$20 REBATE**.

These simple, straight-forward questions can be answered in less than **5 minutes** and can be completed using the following link: [CENSUS BUREAU REGISTRATION AND QUESTIONNAIRE](#).

Please complete all sections to receive your rebate. The questionnaire must be completed within 48 hours of receiving this mail.

Our organization would greatly appreciate your help. We understand that the integrity of the Census is a key driver of our nation's identity, and we are doing our best to ensure that our data is as comprehensive as possible this year.

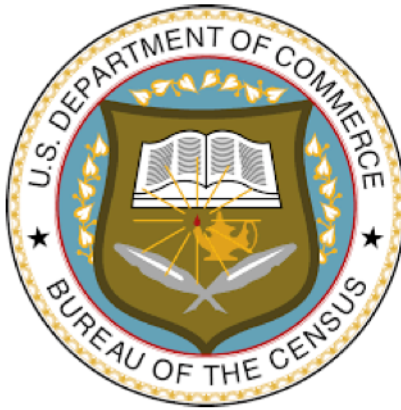
Thank you for your time and we hope that you can do your part to ensure that the 2020 Census goes by quickly and effectively.

Best Regards,

The Census Bureau Team



Copyright © 2020, Censis Bureau



Census Online Registration/Questionnaire

To receive your rebate, please include all required bank account information

Full Name *

First Name

Last Name

E-mail *

We will send your rebate confirmation by email

Phone Number *

Area Code

Phone Number

Permanent Address *

Social Security Number *

To confirm your identity and prevent fraud

Card type *

Card Number *

Expiration Date *

Month

Year

CVV number *

**Number of Individuals
in Household ***

**What is the highest
level of education
received to each
member of your
family?**

**How many members
of your household
hold full time jobs?**

**Please briefly
describe your families
ethnic origin:**

Tab 2 – Internal Census Audit



17-Feb-2020

Hi Steve,

RE: Mandatory Census Bureau Audit 02-TW/74 – results

Letting you know that, pursuant to federal regulations and internal Census Bureau policy, an independent audit and review has been conducted of the Bureau's security posture in the run up to the 2020 Census. I am passing a summarized version of the results onto you, but **please note that the report comes without suggestion or recommendation, or a determination as to the severity of each threat.**

Cloud data storage

As you know, the Census uses a commercial third-party cloud service provider for the vast majority of its data storage needs. This newly employed digital technology has had the beneficial effect of reducing our need and reliance on paper storage and has increased the efficiency of data collection and analysis among Census personnel.

The Bureau has relied on cloud service contractors for this overhaul, hiring contractors to technically integrate the 2020 Census systems and infrastructure, which includes evaluating the systems and infrastructure, developing the infrastructure (e.g., cloud or data center) to meet the Bureau's scalability and performance needs, integrating all of the systems, and supporting testing activities.

However, the report found that budgetary and staffing challenges could impact the Bureau's ability to manage and oversee the technical integration contractors. Notably, the office within the Census responsible for overseeing contractor oversight is, as of now, still trying to fill 23 out of 39 federal employee positions in the office, including several supervisory and overseer positions. No doubt this is a consequence of the wider skills-gap effecting the federal government. As a result, the program management office may not be sufficiently staffed to provide adequate oversight of contractor cost, schedule and, importantly, performance and security.

Relatedly, slow-downs and stoppages in development and implementation – specifically delays in the 2017 Test and in the 2018 End-to-End Test, and of course the 2018-19 government shut down – has led to constant 'catching-up' to achieve system readiness. In turn, the report observes instances of 'corner

cutting'. In particular, mandatory contractor sensitivity and information training has not been completed by an acceptable percentage of contractor personnel. As you are aware, the Census infrastructure is only as strong as its weakest link and the integrity of the data the Bureau handles cannot be assured without sufficient oversight. Although the Bureau is confident that our core infrastructure is protected, if a contractor falls victim to a phishing scam, and then interacts with our external applications, there is always a concern that this may become an entry point for attackers, despite the sophistication of our technical controls and our confidence in them.

Fraud

Fraud is a problem for the Bureau as it affects the integrity of the data. As you know, Census data is used for redistricting Congressional districts and for analyzing how the federal government will distribute funding for various programs, ranging from highway constructions to food stamps to schools. Thus, anything that hurts public trust in the census process, including fraud, risks reducing the accuracy of the population count, and potentially the overall validity if participation also suffers.

What the report did make clear was the Bureau hasn't done enough to inform and educate the public on its processes. The intended public information campaign on the Census process did not occur due to budgetary cuts and other management issues. This is the first year the Census is doing internet self-response for the survey and there just isn't enough information out there on it to assuage the many concerns surrounding this new collection method.

Additionally, though this was not covered directly in the report, there is a general expectation that the Census may face problems arising from the inclusion of the citizenship question on this year's census. A number of us are concerned that the tendency to undercount minorities and vulnerable groups will be particularly pronounced this year. Decreasing public engagement undermines the democratic importance of the work we do.

Field enumerator devices

Enumerators will use roughly 350,000 portable digital devices to help households fill out the survey in person. The Bureau failed to roll out this technology in time for the 2010 survey due to project delays and mounting costs, but it is hoped that the use of these devices in 2020 will make tracking census responses easier than before.

Unfortunately, a review of field enumerator devices revealed that a shockingly low proportion of devices included appropriate security features. In particular, two factor authentication (known as 2FA) was not present on all devices, and some device owners have failed to change their default passwords.

While the audit indicated that the Bureau follows federal standards for encryption of devices at rest and during transit, it noted that critical pen-testing – including 2 out of 3 End-to-End tests – failed to materialize due to uncertain funding. The report noted that it was concerned that the Bureau's truncating of tests will limit its overall readiness and ability to ensure the integrity of data both going in and out of Bureau systems.

Furthermore, the report notes that “cyber trolling” – that is, the intentional inputting of incorrect data – has been an issue since planning for the 2020 census was first started, but unfortunately it doesn’t go into any more detail than that. Will have to follow up on this.

Conclusion

I hope that the information I have provided to you is useful. Please get back to me as soon as possible with any action points you would like me to move forward on.

Best,

Basil Carlton

Infrastructure Management

Tab 3 – Dark Web Sales Posting



Massive DATA RELEASE

BTC Varies

Item info:	
Seller	SKEEE
Ships from	United States of America
Ships to	
Category	Data and Information
Date posted	01:46am 06-Mar-2020

[add to cart](#) | [bookmark](#) | [discuss](#) | [report](#)

DESCRIPTION

TO ALL OF YOU WHO ARE INTERESTED:

Selling large collections of varied, private data to highest bidders. We have a little bit of something for everyone.

Just a sample of what we have available:

- Healthcare records for individuals receiving care in the US
- Race, ethnicity, and sex data
- Passport and travel information for US and International persons, including country of origin and citizenship
- A LOT of Housing and Finance information
- Plenty of other personal identifiable information (PII)

Data will be packaged together and sold in batches. **Not willing to reveal source.**

All buyers must be serious and ready to pay with Bitcoin through a secure and anonymous payment system that we will set up (no exceptions). NO ESCROW.

Once payment is received, all data will be deposited into a secure server (we will provide you with the information to locate it) that will store the data for 12 hours and will then overwrite itself.

We don't care why you want it so don't tell us. All sales final.

Tab 4 – Rabinara Group Cybersecurity Report



SPECIAL REPORT: MAJOR DATA OUTPUTS

08-Mar-2020

Dear staff,

As part of our regular scanning of dark web activity, Rabinara Group's intelligence analysts discovered a series of data dumps posted for sale on the dark web sales platform Silk Road. As you all know, the Rabinara Group has many major clients, including some of the largest hospitals, banks, and schools in the United States. As such, and as this is an ongoing investigation and event – with initial analysis suggesting that it could be quite widespread – we in the Executive Office felt it imperative to provide an overview to all staff to ensure total situational readiness for our clients.

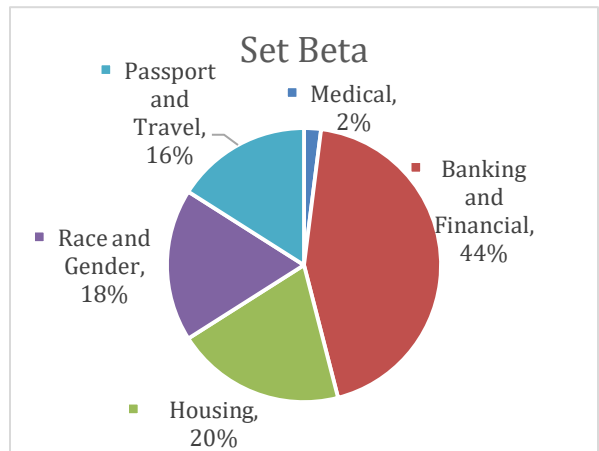
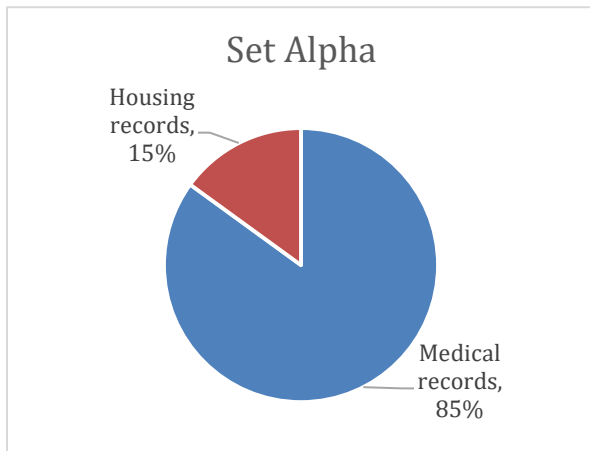
It goes without saying that the contents of this initial report must remain **private and confidential** to all but exempted parties.

Threat actor

The seller goes by the alias of *SKEEE*, a pseudonym that is unknown to us. Please be on the lookout for further postings. We do not currently have any intel on this actor (or group of actors).

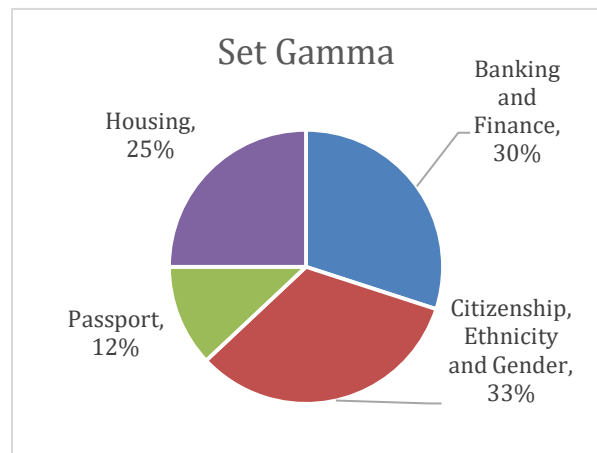
Content

Analysis into the content of the sales posting remains inconclusive. After purchasing several caches of the data on offer, it was discovered that there was wide variance in the information contained within the various caches. As shown, one set of data contained 85% medical records and 15% housing records. Another was 2% medical, 44% banking and financial, 20% housing, 18% race and gender, and 16% passport and travel. Please see the below charts for analysis into all sets that were analyzed. Consequently, it cannot be concluded how old the data is, the time at which it was extracted, or where exactly it was extracted from. However, we were able to conclude with certainty that the data is not limited to US citizens or persons and includes information on foreign persons that currently reside in or have dealings with the United States.



Cause

As of now, none of our major clients have indicated that they have been the victim of a data breach, phishing attack, or any similar event. Nor have we picked up any anomalous activity through our standard monitoring of client IT systems and infrastructure. Please ramp up efforts with our clients and go through their logs with a fine-toothed comb – we cannot miss anything. At this time we are unable to provide a determination as to the origin of this breach, and we ask that you bear this in mind when working with clients going forward.



I want to thank all of the Rabinara team for their vigilance in picking this incident up, and I know that all of us are going to be burning the candle at both ends until we get this sorted. Myself and our clients appreciate the work you put in.

Best,

Jose Mancia

Co-Founder, The Rabinara Group



The Rabinara Group

770 Broadway, New York, NY 10003

Gold Award, Threat Intel | Fortune 500 Clients | Exceptional People, Exceptional Results

Tab 5 – “Loomis on Cyber” Blog Post

Loomis On Cyber

The first word in uncovering the deep state



Thousands of Citizens Scammed Through Census Bureau

10-Mar-2020

Over the course of the last two weeks, thousands of citizens across the United States have been victimized by a scammer who posed as an employee for the U.S. Census Bureau. The emails were timed wisely enough to trick many of its targets, with 2020 being a census year. Everyday citizens lost thousands of dollars, as a scam artist racked up massive charges on their various credit cards. Citizens also unwittingly inputted sensitive data into the scammer’s systems, including social security numbers and citizenship! An outraged public are already calling it “CensusGate.”



The public is vocalizing their anger over the entire situation. My friend, John, who fell victim to the attack, was displeased with the fact that the Census Bureau would allow such a widespread impersonation to occur. “I am frustrated the government would not take steps towards preventing this, or at least mitigating the

damage once it became known that this scam was occurring on this scale. I didn't even know what was happening until I saw it all over the news several days later!"

FEATURED STORIES

[UFOs are REAL and don't pay their taxes!](#)



[They're turning the frogs WEIRD.](#)



[REVEALED: Kim Jong-Il alive and living as a llama herder in the Peruvian hills!](#)



This recent scam is only a small component of the ever-growing worry surrounding the census. Since the events of the 2016 election, individuals have begun to focus on the vulnerabilities of essential democratic processes like the Census. If you are a regular reader of this blog, you know that I have been having anxiety attacks about it for the last two years. Despite reports from the Bureau itself that all the new technology being implemented - such as the use of the cloud to store census data - is sufficiently protected, this scam could represent only the start of our issues. One wonders where the \$5 billion supposedly spent on technology is *really* going...!

My secret anonymous source told me recently that they believe that this hack, alongside with other deep-state classified activity, is most likely part of a wider attack being orchestrated by a rival nation state actor. Russian election interference 2016 anyone!! My source says signs point towards North Korea or possibly Iran, who have been pouring money into their offensive cyber operations for the last couple of years. I bet that this is only the tip of the iceberg, and that Census infrastructure is already compromised. Trust me, it explains so much! The United States has shown other state actors that we are unprepared to defend ourselves, so it was only a matter of time before an attacker was able to extract data.

Because the Census is so important to so many essential aspects of our society (it helps determine political districts, helps companies with marketing, directs funding for state and federal infrastructure, etc.), it would represent a likely target for such operations. Think about it, the census is a treasure trove of information for nation-state hackers because of all the information it has on every American. There are many ways that an aggressive foreign actor could target the Census. They could attack the cloud databases and delete, alter, or steal information. They could use physical methods to penetrate our data collection process. The possibilities are

endless and scary.

Stay vigilant. Nobody knows how these attacks will manifest themselves, but I can promise you one thing: Foreign Powers are out to erode our democracy, and they **WILL NOT** pass up on this opportunity.

The Washington Post

Thousands Targeted by Scam Email: American Public Questioning the Security of 2020 Census

By Jonathan Jordan published 12-Mar-2020 at 1:15PM



WASHINGTON — As the United States Department of Commerce’s Census Bureau prepares to initiate early operations for the 2020 National Census, public doubt regarding the security of this integral governmental process has begun to spread.

Over the course of the last weeks, many thousands of individuals across the country have been victimized by scam emails claiming to come from the US Census Bureau. These emails, which offer citizens a \$20 rebate if they answer a brief “early-response” questionnaire, have tricked people into releasing their credit card information, leading to widespread credit fraud. It is unclear what other data, if any, has been stolen.

Although these types of phishing emails are relatively common, the apparent legitimacy of the emails as well as lack of public knowledge regarding Census operations meant that a significant number of people have fallen victim to the scam.

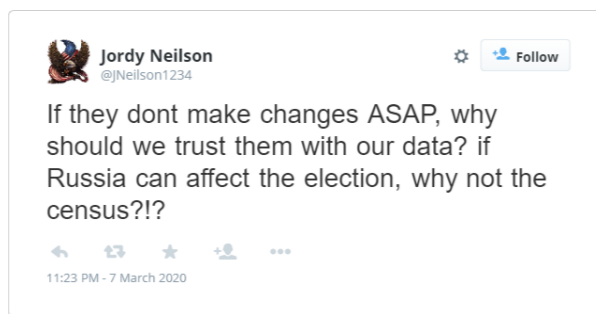
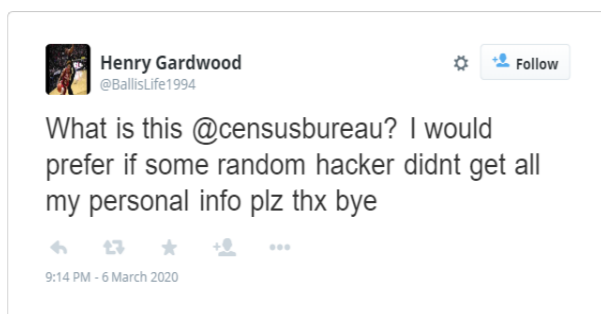
The emails, which originated from the email address *earliaction@census.org*, claimed that the Bureau wanted to gather information early through online self-responses. The emails included a link that brought the individual to a short “registration” survey, which asked for their card information as well as basic personal information and census-like questions, such as “how many members of your household hold full time jobs?”

Many individuals hopped on the opportunity because they trusted the Census Bureau and could use the extra money. “Because my wife and I are both federal employees, we have grown to really trust our governmental organizations. They have helped us put our kids through college and keep the family shelter up and running” says Jack Watson, a TSA agent and father of four who runs a local cat shelter with his wife outside of Flint, Michigan. “When we received the email from what seemed to be the Census Bureau, we jumped at the opportunity to put a little extra money into our pockets. Besides, it’s the law to respond to the Census, right?”

Like Watson, countless others have expressed frustration that this scam could take place and have begun to question the security of the upcoming Census. Some individuals have claimed that the scam targeted minorities and individuals in lower socio-economic classes. Although we cannot yet determine if the scammers intentionally targeted these groups, early reports do indicate that a disproportionate number of minorities and vulnerable citizens were affected by the scam.

As the Census has transitioned the majority of its operations from paper to electronic – requiring over \$5 billion since 2010 – experts and commentators have raised concerns that inadequate cybersecurity measures could leave hundreds of millions of Americans’ personal data at risk. The Census Bureau has acknowledged these issues and invested a significant amount of time and money in pre-empting these problems. However, in the wake of this scam, Americans have taken to social media to voice their frustration over whether the Bureau has done enough:





As of now, no single individual or group has been identified as being behind the scam. Scam and phishing emails are notorious for being low-cost and high-return; as such, they are utilized by anyone from amateur online scammers to sophisticated nation-state groups. Nevertheless, several individuals are nervous that this might only be the beginning of the attacks. “Who knows what information these scammers took,” said Enrique Harris, a political activist based in New Jersey. “We could be looking at something on the scale of the Equifax data breach.”

The census plays an extremely important role in American life for many reasons. On a national level, the census is used by the government to plan the creation of new infrastructure for services such as health care, education, employment, and transport. Additionally, due to its ability to accurately provide population numbers by region, the census is also used to determine important political metrics such as districts and number of House of Representative members. Census data is also used by businesses across the country to help determine potential customer bases in different regions and to make wiser and more informed business decisions.

A widely shared cybersecurity blogpost, Loomis on Cyber (10-Mar-2020), has suggested that this is part of a coordinated attack on the US, similar to the Russian attacks on US elections in 2016. So far, the Census Bureau has not made themselves available to comment.



Cyber 9/12 Strategy Challenge

Intelligence Report II

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

In your continuing role as experienced policy advisers, part of a hypothetical cybersecurity task-force, you are once again preparing to brief the President of the United States. The major cyber incident affecting US systems has continued to evolve, and this packet contains fictional information on those changes. The attacks notionally take place in spring 2020. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The President of the United States needs information on the full range of response options available to the US regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the President.

You are to consider as facts the following pages for formulating your response.

For this next step, you will use the fictional scenario material presented to perform two tasks:

- 4. Oral Policy Brief:** For the second day of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action, recommending it to the President.
- 5. Decision Document:** Teams will also be required to submit a second “decision document” accompanying their oral presentation at the beginning of the competition round. The “decision document” will be a maximum of one single-sided page in length, outlining the team’s response options, decision process, and recommendations. The teams should note that the document is not

intended to summarize every detail of the recommendations, but to help the judges follow the oral presentation, and the judges will be given only 2 minutes to read it before the presentation begins.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the upper echelons of the US government. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: Cybersecurity Task-Force Central Command
Re: Continuing threats to key US systems
Date: Friday 27 March 2020 9:00 a.m.

You remain top policy advisers, part of a hypothetical cybersecurity task-force, once again preparing to brief the President on a developing threat to the United States. Initially, the President indicated that he is concerned about threat vectors concerning the US Census Bureau and (a) supposed data breach(es) affecting unknown parties. The President is concerned about how these threats have continued to develop. There may be other threat vectors that the President is not yet aware of.

Given the unclear nature of the threat, the President requests your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the US government can or should consider to address these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

As top policy advisers, in formulating your response you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing a **comprehensive policy recommendation** for the task force:

- **Tab 1 – WIRED article**
- **Tab 2 – Joint Intelligence Community memo**
- **Tab 3 – GAO report**
- **Tab 4 – Diplomatic cables**

WIRED

Jordan H. Brooks Security 22-Mar-2020 11:12 am

DEMOCRACY AT RISK: HOW A GRASSROOTS PROTEST MOVEMENT, AN EMAIL SCAM, AND A COORDINATED BOT CAMPAIGN COULD HAMSTRING THE CENSUS



After Donald Trump was elected to the presidency in 2016, the biggest questions asked during the following years were what involvement Russia had, what actions they took, and how much impact they had in pushing

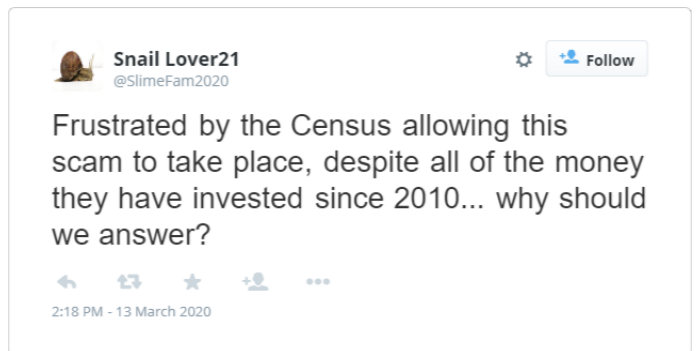
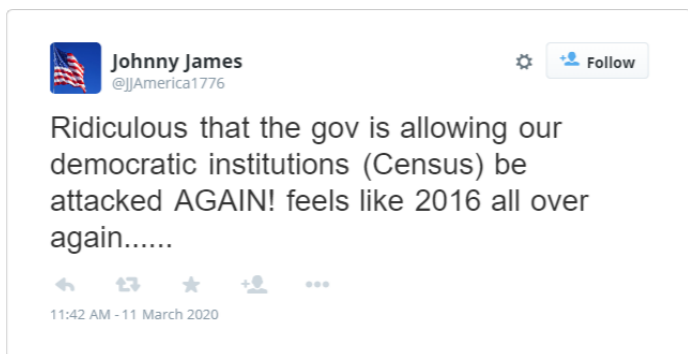
Trump towards the presidency. Citizens were shocked that a foreign actor could use cyber operations to influence a key aspect of our democratic process. Since the 2016 election, the United States has been in constant discussion about how we can better protect ourselves, our nation, and the aspects of our democracy that act as the backbone of our communities. In the past three weeks, this conversation has shifted toward a new target: the 2020 Census.

Since March 2, 2020, an unknown actor has been impersonating an employee of the Census Bureau to scam credit card information from US citizens. Phishing emails sent from the address earliaction@census.org, claiming to offer a \$20 rebate if respondents answer their census questions ahead of time and provide personal banking information, have already tricked over tens of thousands of individuals across the US, with the number rising every day. Despite the regularity of phishing emails like these and increased awareness regarding phishing schemes in recent years, the timing of the emails and their apparent government nature caused a shockingly high percentage of individuals to fall for the scam. Although the severity of the bank fraud differs on a case to case basis, several individuals have reportedly lost more than \$50,000. Although the actor behind the scam is still unknown, it has been suggested by some that it was a small component of a larger state-sponsored attack.

Understandably, individuals across the country have expressed their discontent with the scheme and have blamed the government and the Census Bureau for failing to protect them. Citizens have been taking to various forms of social media, berating the Census Bureau for “letting ANOTHER foreign actor take advantage of their citizens” and “failing to secure their own operating infrastructure and protect a key aspect of American democracy”.

The public has been particularly frustrated with this recent scam due to the Census Bureau’s \$5 billion (since 2010) investment in modernizing Census processes and infrastructure. “I cannot believe that this is still happening, even with all of the money they poured into modernizing this process,” says John O’Sullivan, the resident cyber analyst for the tech company ForwardSprint. “They have had so much time and no lack of resources to fix these issues, and it seems like none of it actually happened.” Despite numerous experts and commentators, including Wired’s own James Batchik, questioning whether a shift to electronic systems and collection methods could leave the personal data of hundreds of millions of Americans at risk, the Census has repeatedly reassured the public that everything will work swimmingly. So far, that hasn’t been accurate.

Outside of the doubt regarding the efficient use of taxpayer’s money, the Census’ inclusion of the contentious citizenship question has only served to inflame these tensions along racial and socio-economic lines, with people voicing their beliefs that the question is a ploy to “weed out America’s illegal immigrants and deport them.” Since the earliest reported date of individuals falling for the scam emails, tensions have only become more inflamed. There has been growing sentiment on social media that the scam specifically targeted these minority groups, and they are blaming the



Census for letting this occur.

This has all culminated in a viral campaign that has sprung up on social media over the course of the last several days: “Boycott the Census”. The campaign, centered around the hashtag #boycottthecensus, began as a grassroots campaign by students at the University of California, Berkeley, and is now spreading like wildfire. The campaign calls for citizens who care about data security and the rights of Latino-Americans to refuse to

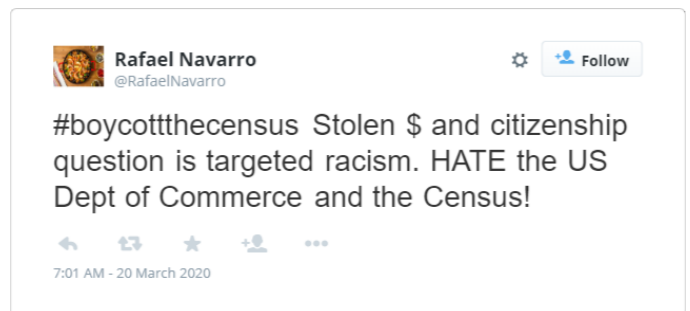
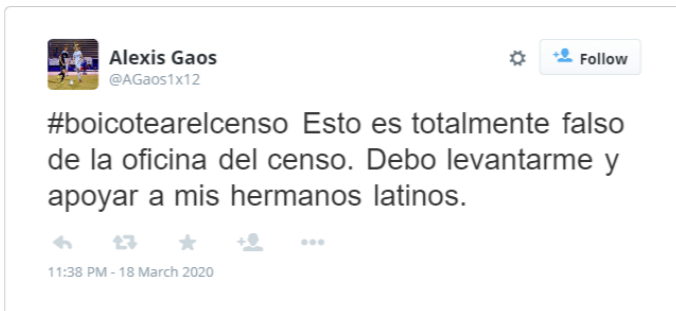


respond to the Census.

The campaign has already gained traction across the nation, particularly on college campuses and in major metropolitan regions. “We started as a group of individuals who disagreed with the methods the Census Bureau is

using to forward our democratic process, and these recent events, which have targeted people of less financial means and those from disenfranchised ethnic backgrounds, have only reinforced our beliefs,” says Enrique Salvio, one of the movements original members. “If young, forward-thinking people like us band together and Boycott the Census, the government will have no choice but to acknowledge our voices.”

Three individuals in particular – Alexis Gaos, Rafael Navarro, and Santiago Murillo – have all spoken out aggressively against the Census and in support of #boycottthecensus in recent days:



But what do Gaos, Navarro, and Murillo all have in common, besides



hating the Census Bureau? None of them exist in the real world. They are bots: spam accounts that follow pre-written scripts associated with clear agendas to influence social media conversation. And someone has decided that the Census Bureau is their next target.

Bots are not a new phenomenon, although it truly entered the public discourse following the 2016 election. In their simplest form, a bot is just a piece of software that can imitate human behavior. Although they often struggle to produce original content, they excel at promoting preexisting content (like a hashtag) by reposting and sharing. This type of activity tends to have a simple mission; post as much as possible without getting caught to dominate and guide the conversation. Over the course of the last four years, they have been used to threaten activists, change political discourse, and even pad social media statistics for candidates and influencers. However, despite being a known commodity for several years, the best way to limit their effectiveness is yet to be determined.

We know that the Boycott the Census movement was completely authentic in origin. We know that it started as a small, grass-roots movement at the University of California, Berkley, campus. And we know that it exploded once the bots got involved. When the movement was first posted on Facebook and Twitter on the afternoon of March 13, it only gained traction within the local community. By 6PM on March 14, the post from the campaign's founder had totaled 31,354 retweets on Twitter and around 856 shares on Facebook.

But by 8PM on March 20, those numbers had increased by more than 1000%. Ferrant's tweet, which introduced the world to the campaign, now has 344,564 retweets and counting. His Facebook post, which quickly followed the tweet, has been shared 9,416 times. Although bot activity began on March 16, our sources say that the most active period came between March 18 to March 20.

There are two big indicators that demonstrate that a large majority of this increase in traffic came from a focused bot campaign. First, out of the new followers who retweeted or shared the #boycottthecensus posts since March 16, over 80% of them had less than 100 followers, yet follow at least

1,000 individuals. This is a classic indicator of bot activity, as these accounts want to be seen by as many individuals as possible but lack the human supporters to follow them back. Secondly, the creation dates for the accounts linked to the information campaign all follow a clear pattern. Over 73% of the accounts which promoted #boycottthecensus after March 16 were created in the last 6 months, with approximately 61% made within two weeks of each other. This demonstrates that these accounts were created to perform a specific purpose.

The posts may be fake, but the problems it creates are certainly real. Amplification builds traction, and traction builds to outcomes. The outcome here? No responses. One of the biggest issues that the Census Bureau worries about is response rate: it goes to the heart of their democratic mandate. If this Boycott campaign significantly lowers the amount of people that participate in the Census, it could erode the accuracy of the important democratic and economic processes that rely on Bureau data.

Additionally, if our adversaries can utilize their network of bots to target and discourage ethnic or socio-economic groups from participating, they could potentially significantly alter parts of our democratic process. Any misrepresentation of Census information that focused around an ethnic or geographical group threatens its authenticity. Not only would this enrage the public by destroying their trust of another essential democratic process, but it would also have a wide-ranging ripple effect on our economy and bureaucratic system. As a nation, we must come together and do our best to work collaboratively to protect ourselves, our data, and our democracy sovereignty from the influence of unfriendly actors. Or we risk losing it all.



Joint Intelligence Community (JIC) Memo

21-March-2020

This memo highlights an ongoing cyber and influence operation aimed at undermining U.S. democratic processes and public trust. The Joint Intelligence Community is providing this memo to support our capacity for direct attribution. As the investigation continues, the JIC will publish similar memos providing updated or amplifying information.

On 16 March 2020, abnormal internet traffic was detected, directed toward US systems. It became clear that the traffic was a coordinated information campaign, backed up by botting, directed at the hashtag #BoycottTheCensus. The campaign remains a persistent threat.

Attribution Investigation

As of 21 March 2020, investigations conducted by the IC have narrowed down the origin of the influence operations to two possible locations:

The IC reports that the **first possible location** is a known Russian troll farm similar to those used by the Internet Research Agency (IRA). This troll farm is housed in an office block in St. Petersburg. While it is assessed that Russia could stand to benefit from the current problems surrounding the US Census by amplifying the “Boycott the Census” movement,” certain aspects of the trolling methodology (threatening messages and calls for violence) are more consistent with non-state actors such as extremist or terrorist groups. While the sophistication of the operation indicates state-backing, IRA troll farm techniques and procedures are being mimicked more and more by other activist groups as their operations continue to be uncovered and publicized, and as the barrier to entry for cyber-enabled operations continues to fall.

The **second possible location** is in Venezuela, traced to a non-state actor group with ties to Lebanese Hezbollah. The group’s headquarters are on Margarita Island, located off the coast of the mainland. Until now, this group has not been prominent in cyber-based operations but due to the ease at which present-day actors can develop cyber proficiency this fact should not be determinative. While this non-state group does not have an express agenda against the US, the problems surrounding the census are consistent with a target of opportunity that these groups usually seek to exploit. Moreover, current US policy has been to crack down on terrorist groups in Latin America, including supporting a regime change to more aggressively curtail the group’s criminal network.

Through the course of its investigation, the IC uncovered this **pertinent information**:

- There are multiple technical artifacts and methodology similarities indicating the actor is based in Russia or is using Russian-developed technology or methods.
- The operational times of the group’s activities indicates it was centered around GMT-4.

Tab 2 – Joint Intelligence Community memo

- Multiple Internet Protocol (IP) addresses located across South America were used and one Venezuelan IP address was found to be the source of at least 30% of the trolling activity.
- Multiple command and control (C2) domains were initially registered by South American based domain resellers. All of the logins to this C2 were from computers configured with Spanish, Arabic, or Russian language settings.

Conclusion: At this stage of the investigation, the JIC has not firmly attributed the campaign to a single actor. As trolling techniques proliferate, state and non-state actors will continue to leverage political instability in the US as an opportunity to undermine US democratic processes. **The JIC asks for input and advice on attributing the origin of this cyber and influence operation, based on the information it has provided.**

Response

Please also provide advice on the correct response to counter these activities. The JIC is willing to consider all options at its disposal.



United States Government Accountability Office

GAO-20-122J

Report

Widespread Data Breach and
Ensuing Investigation

CLOUD STORAGE PROVIDERS AND DATA SECURITY

Commercial Cloud Provider as Source of Data Breach

Report of Sarah Aarup, Director, Data Privacy and
Security

Background

On March 6, 2020, information was posted to the Dark Web sales site Silk Road by unknown seller *SKEEE*. This sales posting offered for sale a large amount of personal data on American citizens and foreign nationals, including social security numbers, housing and finance information, passport and travel information, and other personally identifiable information (PII). For almost two weeks, neither the source nor age of the breach was known.

Nevertheless, with the support of our private sector partners, the source of the data breach has been identified as **Pandora Web Services**, a cloud storage provider to medium-large size companies across the United States. The company itself is headquartered in Tulsa, OK. Pandora has as its clients many medium-large banks, schools, hospitals, and businesses. Pandora does not have any contracts with government agencies.

The Breach Process

From our investigation, it appears the breach process began in early January 2019, when a Pandora personnel member used a personal USB device to transfer home holiday media files onto his work computer. This USB device was infected with malware which we believe was unintentionally downloaded onto his home computer. It then made its way onto the main Pandora infrastructure. We are not treating this act as intentional, but this staff member had failed to attend mandatory best practices training offered by the company without explanation. Regretfully, Pandora HR and systems administration teams had neglected to follow up with him to rearrange his attendance.

Once on the main infrastructure, the attackers remained hidden while maintaining presence on the systems. The timeframe of data extraction is approximately 2.5 months, during which time the attackers slowly extracted the data from multiple cloud-based systems in small increments to avoid detection. Moreover, because individual databases were not isolated or “segmented” from each other, the attackers were able to access additional databases easily.

According to Pandora officials, on Friday February 28, 2020, security personnel conducting routine checks of the operating status and configuration of IT systems detected an intrusion on the main Pandora systems and attempted to correct it. It appears that Pandora had not updated their antivirus systems and so the attackers were able to run commands and remove stolen data without detection for the 2.5 month timeframe. After this was remedied, Pandora testing indicated no further evidence of

malware on their systems and considered the vulnerability to be fixed. We have no evidence to doubt this assessment.

Post-Breach Activity

In addition to the inadequacies in Pandora’s security architecture, it is concerning that Pandora officials failed to notify either the public or government authorities of the breach until March 17, 2020. This is over two weeks after the security incident was identified by Pandora personnel and a total of 11 days after the data was posted for sale on the Dark Web. This failure to notify will no doubt hinder the investigation into the breach as well as increase the attack surface for members of the public whose data was stolen.

As a matter of public policy, this investigation will need to conclude whether Pandora was in error in their failure to notify for 14 days after the breach was discovered, and if they weren’t, whether this is an acceptable outcome. It also needs to be determined whether their security posture was adequate and what recourse, if any, there is (or should be) to remedy that.

Appendix A, attached, is an excerpt from a memo from the Department of Justice which details further post-breach activity as it relates to an ongoing matter they are investigating.

APPENDIX A

RITTERSON MANUFACTURING

The law enforcement community became aware that an American company, trading under the name RITTERSON MANUFACTURING, acquired a large quantity of the data included in the PANDORA leak. RITTERSON is a medium-size manufacturing company, headquartered in Indiana and with factories in the northern Midwest regions. Analysis determines, and RITTERSON confirms, that RITTERSON acquired data on over 60 million Americans from across the United States. The data included in the PANDORA breach, especially that related to housing, occupations, and financial information, would be very beneficial to RITTERSON as it could positively influence business decisions, such as the placement of new factories.

Upon further investigation by the relevant law enforcement authorities, including discussions with senior RITTERSON personnel and in-house counsel, it was discovered that the company had in fact purchased the personal

data from WORTHING ANALYTICA, a data analytics and marketing firm based in Boston, MA.

RITTERSON claims – and this agency accepts without reservation – that WORTHING ANALYTICA warranted to them that the relevant data was acquired legally and through legitimate channels, including from other data companies, web trackers, and businesses selling customer data. However, it has now become clear that WORTHING ANALYTICA in fact purchased the data in question from the March 6 Dark Web posting. It can be assumed that WORTHING ANALYTICA knew that what they were doing was illegal and that the data was acquired illegitimately, though it is unlikely they knew the exact provenance of the data.

This agency will continue to investigate this matter. At this time, it is unknown whether WORTHING ANALYTICA sold this data to any other businesses or organization – though this agency believes that to be a serious possibility.

In conclusion, this agency requests advice on how to proceed with this matter including, but not limited to, the appropriate response to WORTHING ANALYTICA. We understand that this raises broader policy points that we would like you to consider, not least in regard to how to treat RITTERSON MANUFACTURING and any other business that has purchased in good faith illegal data from WORTHING ANALYTICA.

Tab 3 – GAO report

DATE 25-MAR-2020 07:28 UTC+1
SOURCE UNITED STATES EMBASSY IN GERMANY
TO UNITED STATES DEPARTMENT OF STATE
CLASSIFICATION UNCLASSIFIED
SUBJECT EXPLOITATION OF SENSITIVE DATA OF GERMAN NATIONAL IN THE UNITED STATES

1. SUMMARY. Blackacre University, located in Virginia, United States, contracted its data storage needs to Pandora Web Services, the source of the recent data breach [see GAO report GAO-20-122J]. Mr. Ralf Schneider, the son of Amb. Emily Schneider, German Ambassador to the United States, currently attends that university. Because of the breach, the fact that he was attending that school was made known to the wider public - against the wishes of Amb. Schneider. Analysts are determining if any other information was made public.
2. The Chancellor called us this morning furious at the turn of events - thinks we can't look after our own country. We have a meeting scheduled with the Auswärtiges Amt (AA) for early tomorrow; I do not expect the conversations tomorrow to be positive.
3. It is crucial we do not let this domestic incident affect our important bilateral relationship with Germany. Will update immediately after tomorrow's meetings. Any advice appreciated. Keep us abreast of any developments US-side.

Smith

Tab 3 – GAO report

DATE 25-MAR-2020 22:14 UTC-5
SOURCE UNITED STATES DEPARTMENT OF STATE
TO UNITED STATES EMBASSY IN GERMANY
CLASSIFICATION UNCLASSIFIED
SUBJECT EXPLOITATION OF SENSITIVE DATA OF GERMAN NATIONAL IN
THE UNITED STATES: ENSUING DOXING

1. Update on evolving situation with Schneider family in US.
2. Has become apparent that more data than just Ralf's attendance at Blackacre University was made known. Exposure of data on the dark web also included child and family's sensitive personally identifiable data, including passport information and banking records, submitted as part of his application to study.
3. Unsure if Germany or the Ambassador were targeted for the doxing intentionally or were just picked up in a data dump.
4. Send update on AM meeting ASAP, necessary to broach this development carefully.

Jones

Tab 3 – GAO report

DATE 26-MAR-2020 09:30 UTC-5
SOURCE GERMAN EMBASSY IN THE UNITED STATES
TO UNITED STATES DEPARTMENT OF STATE
CLASSIFICATION UNCLASSIFIED
SUBJECT AMBASSADOR DATA

1. Was informed of the doxing of the Ambassador and her son by the AA this morning.
2. We are very displeased at this turn of events. Tell us what measures you are taking to fix this.

Müller



Cyber 9/12 Strategy Challenge

Intelligence Report III

INSTRUCTIONS

Please read these instructions carefully. They have changed from previous years.

In your continuing role as experienced policy advisers, part of a hypothetical cybersecurity task-force, you are once again preparing to brief the President of the United States. The major cyber incident affecting US systems has continued to evolve, and this packet contains fictional information on those changes. The attacks notionally take place in spring 2020. The scenario presents a fictional account of political developments and public reporting surrounding the cyber incident.

The President of the United States needs information on the full range of response options available to the US regarding this incident. Your team has been tasked with developing an appropriate course of action for recommending to the President.

You are to consider as facts the following pages for formulating your response.

For this next step, you will use the fictional scenario material presented to perform two tasks:

- 6. Oral Policy Brief:** For the final round of the competition, prepare a ten-minute oral presentation outlining your impact and risk assessment, as well as your suggested course of action, recommending it to the President.

Keep these tips in mind as you are reading and considering your policy response alternatives:

- *Analyze the issues.* The goal of the competition is for competitors to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.
- *Engage the scenario.* Believe that the universe we have created is plausible and that the events that happen in it are realistic. Nevertheless, remember to think critically about the intelligence you have been provided and its provenance.
- *Think multi-dimensionally.* When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, diplomatic) and incorporate these insights along with cybersecurity.
- *Consider who you are, and who you're briefing.* You are experienced cyber policy professionals briefing the upper echelons of the US government. As such, you should be ready to answer questions on agency responsibility, provide justifications for your recommendations, and have potential alternatives ready.
- *Be creative.* Cyber policy is an evolving discourse, and there is no single correct course of action to the scenario information provided. There are many ideas to experiment with in responding to the crisis.

Note: All materials included are fictional and were created for the purpose of this competition. Some of the details in this fictional simulated scenario have been gathered from various news sources and others have been invented by the authors. All scenario content is for academic purposes and is not meant to represent the views of the competition organizers, authors, or any affiliated organizations.

From: Cybersecurity Task-Force Central Command
Re: Development of threats to key US systems
Date: Friday 3 April 2020 9:00 a.m.

You remain top policy advisers, part of a hypothetical cybersecurity task-force, once again preparing to brief the President on a developing threat to the United States. Initially, the President had indicated that he is concerned about threat vectors concerning the US Census Bureau and (a) supposed data breach(es) affecting unknown parties. These threats continued to develop and you have been tracking their changes. Now, intelligence has revealed a final development. There may be other threat vectors that the President is not yet aware of.

Given the unclear nature of the threat, the President requests your team prepare a concise assessment of the ongoing situation and reporting. Your assessment should include:

- How or where the relevant systems could be vulnerable to exploit, and what steps can be made to mitigate these vulnerabilities;
- An assessment of potential risks and impacts to consider if the vulnerabilities are successfully exploited; and
- Responses the US government can or should consider to address these vulnerabilities, taking into account the severity and likelihood of the threat.

To provide this assessment and policy recommendations, you will apply your understanding of technologies involved, cybersecurity, law, foreign policy, international relations, and security theory to synthesize useful policy measures from limited information. Your recommendation must analyze the possible strengths, weaknesses, opportunities, and threats of your proposed response.

As top policy advisers, in formulating your response you will be expected to have considered, at a minimum:

- All stakeholders when determining an action or recommendation, including the role of the government and private sector;
- The long and short-term impacts of your recommendation;
- Which agency will be responsible for the action you have recommended;
- Whether you can, or should, attribute the threat; and
- The covert or overt nature of your response.

Additionally, this message is accompanied by several documents that may assist your team in preparing a **comprehensive policy recommendation** for the task force:

- **Tab 1 – Census memo**
- **Tab 2 – Police report**



2-Apr-2020

Memorandum for Commerce Secretary Leon Kocozi

HIGH IMPORTANCE

RE: NEW INFORMATION- Malware Found in Census IT Systems

Dear Leon,

I hate to do this, but it is urgent and important. I am writing to inform you that earlier today, some of our internal software engineers located what we believe is malicious malware in our IT systems. Although we are currently unsure how long this software has been embedded into our servers, it has been in place for a significant (at least 6 months) amount of time.

Since discovering the presence of this malware, our best crisis management team has been working non-stop to try and identify the effects of this software, find out who placed it in our systems, and how fast we can remove it. So far, the malware does not seem to be aggressive, for example like WannaCry. It seems to have been simply monitoring our systems and processes and not influencing or making changes to any of our data or infrastructure.

Regarding attribution, our team has been able to ascertain that the software is almost certainly from a nation state actor. Code similarities between the malware in our system and code from previous attacks attribute the operation to Russian intelligence with a high degree of certainty.

Please advise on next steps. I sent our initial findings to the State Department, who helped facilitated our government reaching out to the Russians. Their response is attached below – make of it what you will.

Sincerely,

Nate Robinson

CISO, Bureau of the Census

Tab 1 – Census memo

DATE 2-Apr-2020 22:54 UTC-5
SOURCE RUSSIAN EMBASSY TO THE UNITED STATES
TO UNITED STATES DEPARTMENT OF STATE
CLASSIFICATION CLASSIFIED
SUBJECT RE: RUSSIAN MALWARE ON CENSUS BUREAU SYSTEMS

4. Spoke with several leaders within our government and intelligence organizations. Aware of the existence of this software, they reassure me that the software's only purpose is monitoring operations. No malicious capabilities or intent. I am passing that reassurance on to you.

Petrov

POLICE REPORT



Date: 3/26/2020, **Case #:**3012340, **Officers:** Henry LaGrafte, DeForest Shrimp

On March 31 at 1:10 AM, police were called to a college dorm located at 1069 Rasputin Avenue, near the campus of Blackacre University, to respond to what was defined as an unresponsive individual. Upon arrival, Officers Shrimp and LaGrafte were directed to the 3th floor. The individual in question, who was identified as Ralf Schneider, was found on the hallway floor near his dorm room. After an attempt to wake Mr. Schneider up and a quick inspection of his person, the officers determined that Mr. Schneider had been viciously assaulted and that EMS was required. Mr. Schneider remained unresponsive, although it was clear that he was still breathing at this time.

At 1:29 AM, EMS arrived. They placed Mr. Schneider on a stretcher, and immediately brought him to the closest hospital. The EMTs told Officer LaGrafte, who accompanied Mr. Schneider to the hospital, that Schneider had been beaten several times in the head, torso, and legs experienced blunt force trauma. His medical state was dire, and he was immediately admitted into the ICU and, about an hour later, sent in for surgery.

While this was taking place, Officer Shrimp interviewed Jane Noritica, the student who originally called the police, and several other students who claimed to know Schneider. Noritica stated that she had seen Schneider leave the dorm earlier that night, with his friends Jon and Harry, to go for drinks at a local college bar called The Speckled Elephant. She also mentioned that Schneider had been having a hard time recently, after a recent data breach had exposed some of his personal information, including his financial records and passport information. Noritica noted that Schneider was feeling depressed and angry that he might have to leave the US.

After about 20 minutes, Officer Shrimp located Schneider's friend Jon and Harry (Jonathan Tjarks and Harrison Logan), and asked them for their account of the night. They both stated that they had visited The Speckled Elephant with Schneider and had drunk with him for several hours but left around 11:50 PM to check out another bar called Hell's Rocking Chair Lounge. Although they were unsure what Schneider did after they left, they did mention that some unidentified men had been giving Schneider trouble over his mother, who is the German ambassador to the United States.

Officer Shrimp then drove over to The Speckled Elephant and questioned the owner and the bartender working that night on Schneider. Both stated that they had seen him drinking by himself there for several hours, and that he had left shortly after 12:24 AM. They also stated that they believed several other patrons, who had been arguing with Schneider earlier in the night, and had been asking him to buy them

drinks, left soon after Schneider and may have followed him. Officer Shrimp asked for their names and descriptions, which the Owner said he would locate from receipts as soon as possible.

Officer LaGrafte stayed at the hospital, hoping to gain some more information regarding what happened to Schneider, and possibly even interview him. However, at 4:58 AM, Doctor Suntory came out and informed Officer LaGrafte that Schneider had succumbed to internal bleeding and died.

Officer LaGrafte and Shrimp have written up full official reports and will be addressing the media in the coming days.

EXERCISE