STATEMENT
of
Kevin Smith
Associate Director and Chief Information Officer
of the U.S. Census Bureau
Before the
U.S. House of Representatives
House Oversight and Government Reform Committee,
Subcommittee on Government Operations

Chairman Meadows, Ranking Member Connolly and members of the Subcommittee, thank you for the opportunity to testify this afternoon. I am pleased to update you on the status and ongoing work to ensure the success of the 2020 Census.

I began my role as Chief Information Officer of the Census Bureau over four months ago. Since then, I have gained a deep appreciation of the visionary steps the agency has taken to introduce innovations into their operational processes and supporting technology to make the 2020 Census more effective and efficient than ever before. The tight connection between technological capabilities and operational processes is clear, and demonstrates the need to have the right level of technology in place to support the operational tests for the 2020 Census. The Census Bureau has taken positive steps to *innovate* with technology – not *invent* technology – by utilizing industry available solutions wherever possible. I have been involved in developing first-of-their-kind industry solutions and large-scale technology modernization efforts in both government and the private sector. I am excited and honored to lead the IT team that will help deliver the most automated census ever.

I am under no illusions that the task before us is an easy one; in fact, it is very difficult. I have spent much of my time at the Census Bureau reviewing the IT organization, as well as the technology, governance and innovation processes that are currently in place. My observations are that the foundation to carry out a successful census is in place.

However, we still have a lot of work ahead of us. I would like to focus on two key areas: our cybersecurity approach to ensuring the integrity and security of our systems and data, and the progress of the Census Enterprise Data Collection and Processing (CEDCaP) program.

Our cybersecurity approach will ensure that individuals have limited and appropriate access to 2020 Census data by developing redundant systems with layers, isolation, encryption, and views that enable us to act according to possible threats. For example, within the Census Bureau we conduct our cybersecurity awareness training and phishing evaluations to educate our employees. We have also worked with the U.S. Department of Homeland Security (DHS) to evaluate and test our procedures for phishing. This will enable us to find and fix potential vulnerabilities before a compromise occurs. On enumerators' mobile devices, we are using two-factor authentication, encrypting data at rest and in transit.

We take the task of ensuring the integrity and security of our systems and data against the ever-evolving landscape of cybersecurity threats very seriously. We have engaged industry and other Federal agencies, most prominently DHS (Cybersecurity Assurance Branch – Federal Network Resilience), to assist us in reviewing our design and security architecture for the 2020 Census systems. In addition, we have reached out to the National Security Agency (NSA) (Customer Advocate and Information Assurance Sections) and other offices within the Department of Commerce (DOC) (Investigations and Threat Management Division) for assistance in threat identification and management.

The Census Bureau also works very closely with the Department of Commerce Office of the Chief Information Office (OCIO).   The coordination between Census and the Department has been seamless and significant. Incident response, the Enterprise Security Operations Center (ESOC), High Value Asset (HVA) assessments and Continuous Diagnostic and Mitigation are areas where the Department has improved cybersecurity on behalf of Census.   In addition, the implementation of FITARA within Census has provided a greater level of visibility for Census investments at the Department.

We are already using recognized cybersecurity services from DHS and industry. The Census Bureau uses and supports the DHS programs for EINSTEIN, employing EINSTEIN 3 Accelerated, and Continuous Diagnostics and Mitigation (CDM). We use cloud and internet service providers to protect against Distributed Denial of Service (DDoS) attacks. Within our infrastructure, we have additional security at the perimeter and internally to ensure the protection of Census Bureau data, as discussed in previous hearings. We are committed to continuing to partner with industry and other Federal agencies to use cybersecurity services throughout multiple layers of our systems. This will create as strong a cybersecurity posture as possible to advance our visibility and protection against these evolving threats.

The Census Bureau's IT and cybersecurity program provides protection to not only our IT infrastructure and systems. More importantly, it protects the personal and business information we collect from our respondents, and the administrative data we receive from other agencies to support our mission. I am very confident in our ability to protect the information and information systems through our current policies and processes. We will continue to enhance those policies and processes as we implement new tools and technologies to address the evolving threat environment.

Current Environment

The Census Bureau environment currently consists of 29 uniquely defined, Federal Information Security Act (FISMA) reportable systems. These systems are comprised of 542 technology components, such as physical security, environmental, centralized identification management, backup, etc. Program areas can use these components to reduce the cost and time to assess their systems, as well as reduce the overall IT management responsibilities for which their staff are responsible.

To secure this environment, our IT/cybersecurity program is multi-dimensional, multi-level, and multi-governed. We look at all aspects of the Census Bureau's mission and determine how to provide the security needed to successfully accomplish that mission, while providing a high level of confidence to our respondents and partner agencies.

<u>Multi-dimensional</u>

Our IT/cybersecurity program looks at people; physical security; infrastructure; IT systems; how our IT systems interface with other systems (both inside the Census Bureau as well as externally); the applications used to collect and process the information; and the data themselves.

People – People are perhaps the most important component of this multi-dimensional process. They can be the strongest link we have to ensure our systems and data security by implementing appropriate security controls and ensuring they are operating as intended. People can also be the weakest link – by committing human error in system administration, database administration, or programming, by becoming victims of phishing scams, or by visiting malware-infected internet sites. We require certain levels of security to be in place prior to allowing people – whether employees or contractors – to access our IT systems. We also require background investigations appropriate to the position sensitivity, the issuance of a multi-factor ID card that is required to access the network, authorization to individual systems and accounts, and regular awareness training.

Threats may also originate from people within the organization, “insiders” such as employees, former employees, contractors or business associates, who have information concerning the organization's security practices, data and computer systems. Recognizing this potential threat, the Census Bureau has engaged with the Insider Threat Center at Carnegie Mellon University to review our current posture and recommend areas where we can strengthen the program. The Census Bureau will use these and future discussions with Carnegie Mellon to improve our insider threat program to provide additional protection to the data we collect, process and disseminate.

Physical security – We make sure that our people, systems, and data are protected from physical threats. In coordination with the Office of Security, we review the IT security controls in place. This includes the application of Interagency Security Committee standards for physical access to buildings, physical access controls to sensitive spaces such as server rooms, and continuing security education.

Infrastructure – Our infrastructure is key to mission success. This includes the environmental controls at our Bowie Computer Center and the National Processing Center, and our redundant telecommunications infrastructure that provides automatic failover to make sure that we can complete our mission successfully and securely. Some examples of the infrastructure security tools we use include the security assessment and monitoring of processes, routers, switches, firewalls and our load balancers.

IT systems – IT systems are defined as servers, PCs, storage, databases, laptops, mobile devices, etc. These are all assessed and must have a formal approval to operate, whether internally at the Census Bureau or externally at a contractor site or in the cloud environment. The Office of Information Security (OIS) uses the Risk Management Framework to ensure the required security controls are in place and assessed prior to any authorization. OIS also assigns IT Security Engineers to support Census Bureau IT projects during all phases of the system development life cycle. Additionally, each system is assigned an Information System Security Officer (ISSO) who is assigned to the OIS and directly supports the System Owner. The ISSO works closely with the System Owner prior to and following the formal authorization process, and ensures the security remains in place and effective while the system is in production. Each system has a secure configuration baseline in place. This baseline and security patches are checked each month through automated scanning.

Interfaces – In addition to assessing the servers, databases, and storage individually, the interfaces needed for these IT resources to work with each other securely and efficiently are documented and reviewed by IT security staff, the System Owners, and Authorizing Officials.

Applications – Applications are the lynchpin to any IT system's ability to successfully support its mission as intended. Applications are also becoming a favored, if not the most favored, point of attack. This threat is increasing for a variety of reasons, but primarily we are getting much better at hardening our systems and databases at the core level. On the other hand, applications are developed by people – either employees or contractors of the Census Bureau, or through a commercial off the shelf (COTS) product. To address this, we scan the application code of our internet-facing web applications on a regular basis, based on risk.

Data - The Census Bureau's mission is to serve as the leading source of quality data about the Nation's people and economy. Our data are an essential component of that mission. If we do not protect data, we cannot maintain the level of trust we need for respondents and our partners to provide us their information. Data are the most important element of our multi-dimensional IT/cybersecurity program; all the other areas provide protection to this core element. Our data are contained in databases or in our storage and backup processes, and we provide the security at those levels. We also use the process of 'least privilege' to ensure that only the appropriate, authorized people actually have access to it – and only for mission-related purposes. We have approved a design pattern to require data to be encrypted in transit and at rest. We verify that databases meet the encryption requirement, or have a formal Plan of Action and Milestone to ensure that they will. We monitor this through formal access control permissions, auditing, and continuous monitoring. We continue to look at additional automated tools to provide protection from potential insider threat to our systems or data.

Continuous Improvement

The cyber threat continues to grow and evolve, especially as we rely more on emerging technologies like the cloud and social media, and as we use more open, transparent processes and reengineer and modernize our operations. To meet this growing challenge, our IT/cybersecurity program must continue to grow and evolve as well. We must continually develop the controls and processes to address our adversaries' intentions to steal our data or disrupt our operations, while maintaining a balance that provides for the successful completion of our core mission.

The Census Bureau takes seriously its responsibility to protect respondent data and is engaged in this regard on a number of cybersecurity and technology fronts:

Phishing

The U.S. Government Accountability Office (GAO) identified a few key cybersecurity areas in its latest report (released September 8, 2016). In particular, GAO raised concerns surrounding the Census Bureau's approach to minimizing the threat of phishing and ensuring appropriate access to 2020 Census data, while having adequate controls for internet data collection systems supported in a cloud environment. Similar to our approach in 2010, the Census will use an industry leading company, MarkMonitor, to provide brand and fraud protection on the internet by detecting rogue and suspect emails and websites impersonating the Census Bureau. This service will help preserve the Census Bureau's public presence by helping to eliminate fraudulent impersonations of the Census Bureau online. The service continuously monitors web traffic for potential brand abuse, such as unauthorized domains or websites; false associations; brand impersonations; cybersquatting; and other threats. We also use a service that inspects email traffic sent to ensure that others are not attempting to pass themselves off as the Census Bureau via email. The service compares technical information in the email traffic to validate it.

The Census Bureau is implementing several additional strategies to protect against phishing scams. First, we are developing an internal communications plan to reinforce our employees' understanding of security awareness and their role in protecting the Census Bureau. Second, we are working with the Integrated Communications Contract for the 2020 Decennial Census to develop messages and communication tools for the public on phishing and other cybersecurity threats. We are increasing our use of the PhishMe service to conduct regular anti-phishing exercises for all Census Bureau employees and contractors. Finally, we have acquired a technology that will 'detonate' attachments and links embedded in emails in a 'sandbox' environment, to keep them from reaching the Census Bureau network. We are currently working to implement this within the infrastructure.

Access Management

The Census Bureau is implementing layered protection for our internet data collection system. We are exploring several strategies, including the possibility of distributing applications across multiple cloud vendors, so that security issues in one layer would not affect the entire system. We are also working within the Census Bureau to reinforce business rules for incident handling, including escalation and decision points, and to ensure that they are clearly documented and well understood across the agency.

Mobile

The Census Bureau plans to deploy mobile solutions in support of the 2020 Census. We employ a range of security measures to protect our systems and data on mobile platforms. We currently use AirWatch as the Mobile Application Manager (MAM). The MAM allows us to manage Census Bureau applications, make changes to them when needed, ensure the security settings of the application, and wipe applications remotely if necessary. Further, Census Bureau enumerators use a six-digit PIN to access the device, and a 10 character password to authenticate to the application. Data are encrypted at rest on the device, and collected information is transmitted as soon as the case is closed and the device is connected to the internet. Finally, data are transmitted via secure protocols from the field to the Census Bureau.

Cloud

The advent of cloud services provides us with an opportunity, as well as some security challenges. Cloud services and providers must be FedRAMP certified. Additionally, cloud implementations must meet all Census Bureau security requirements for sensitive data. To provide additional assurances, we leverage other government agencies (DHS, NSA, DOC Office of Security Supply Chain Risk Assessment staff, etc.) to review security architecture and assist in testing. We also plan to engage in independent testing, by government agencies as well as contractors, during the FY 2018 test to explore options for fraud protection. Finally, as with any Federal IT system, we must ensure that continuous monitoring is conducted on Cloud solutions, as required by FISMA and FedRAMP.

CEDCaP

The CEDCaP program has been underway since 2015. CEDCaP follows standard enterprise processes for systems development, and some components have already been deployed into production. While much work remains, we are pleased with our efforts to date and remain on schedule for a successful 2020 Census. We have begun the process to configure business rules and models for the 2020 Census, while building the base enterprise capabilities that can be extended for use by other programs.

In May 2016, the Census Bureau announced a decision to unify the functions of a number of existing systems onto a single platform-based COTS solution. This covered our major operational control, internet self-response, address listing and mapping, case management, and mobile collection and management applications, among several others. This hybrid COTS solution will address the short-term goal of deploying the 2020 Census, and build the infrastructure to transition to the long-term goal of CEDCaP's future state to support all surveys and censuses.

The transition to the COTS platform for the 2020 Census began in June 2016 with the formation of the transition team and new 2020 Census development teams, supported by the platform vendor. We quickly updated the 2020 Census Integration and Implementation Plan, 2020 Census Transition Plan, and the CEDCaP Transition Plan to reflect the required readiness dates for test, production, and operations. The CEDCaP systems are built using an Agile Development approach that allows us to work closely together with the Decennial business product owners to improve our ability to deliver the right level of technology. This approach will continually build upon previously released capabilities to iteratively make the most effective improvements for the

Census. The teams are hard at work, and, before the end of the calendar year we will begin end-to-end thread testing for all systems of the 2017 Census Test.

The 2020 Census schedule is integrated with all supporting programs, including CEDCaP. The 2020 Census Program Integrated Master Schedule drives the schedule for all corporate service providers that support the program based on the 2020 Census Program key milestones. The 2020 Census Integrated Master Schedule is the single schedule into which all projects – including enterprise solutions like CEDCaP and the Center for Enterprise Dissemination Services and Consumer Innovation (CEDSCI) – provide weekly status reports. Project teams have their own detailed schedules to support day-to-day tasks that are linked to the integrated master schedule. Because of its complexity, the 2020 Census Program integrated master schedule is developed and maintained using Primavera scheduling software, which meets the required capabilities recommended by GAO. On a monthly basis, the Census Bureau shares the updated integrated master schedule with GAO.

The 2020 Census/CEDCaP schedule integration has taken positive steps to manage the interdependencies between these programs, as acknowledged by GAO. We agree that the Census Bureau must maintain schedule alignment between the 2020 Census and CEDCaP through a single integrated dependency schedule, and we align key milestones and update statuses between the programs weekly. GAO recommends additional actions to better align the programs, such as having an integrated list of all interdependent risks, and finalizing a processes for managing requirements. We already maintain a comprehensive risk register for the 2020 Census and its dependent project level solutions, including CEDCaP. This risk register undergoes regular reviews at the program level, and quarterly reviews by Census Bureau senior leadership, to examine and monitor the highest-level, crosscutting risks. As GAO noted, we have drafted an enterprise requirements management plan and we are currently following that process. We are completing the final reviews of the supporting documentation, and it will be completed by the January 2017 deadline set out in GAO's report.

The CEDCaP program is working to address GAO's additional recommendation in its report "Better Management of Interdependencies between Programs Supporting 2020 Census Is Needed," released on September 8, 2016. We agree with GAO's assertion that the program office estimate needs to be updated, and have developed a plan to do so and begun that effort.

CEDCaP will follow the *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs* when producing annual updates to the program office estimate. We also agree with the GAO's recommendation that we must improve the CEDCaP risk management process used by all the projects. Over the past several months, we have updated the CEDCaP Risk Management Plan and the corresponding standard operating procedures. The established plans and standard operating procedures identify roles and responsibilities for risk management. We established a risk team that assists the projects and risk owners with implementing their risk management process, including documenting risks with trigger dates and completing the detailed mitigation plans for all high risks. The team also audits each project risk register monthly to validate that the risks are properly documented, monitored, and updated.

Looking ahead, in my opinion, the measures we are taking will prepare us to react to any difficulty, and to predict incidents such as cyber attacks. Preserving the integrity and security of our systems and data is a top priority. First, we will protect the data we have already collected, and second, we will sustain secure data collection services so that respondents may continue to confidently provide responses to the 2020 Census. To do that, we will layer our technology in ways that isolate data and systems from each other, with views that let us take the appropriate and immediate action when a threat is detected. We are looking at designing our system to use multiple cloud providers, so there is no single point of failure in the architecture. We are separating out the individual processes into layers, so we can address specific security controls and decision points independently. We have strengthened our work with other agencies to assist in reviewing the security architecture and design of the system, and we are seeking assistance from DHS and NSA to help with penetration testing on the new CEDCaP COTS platform. Finally, we are looking into hiring an independent organization to help test vulnerability to fraud in the non-ID response process during the 2018 End-to-End Census Test. GAO has recently noted the importance of engaging service providers and the IT vendor community to help mitigate risk, and I completely agree with its recommendation.

I would be remiss if I did not mention how impressed I am with the personnel at the Census Bureau. We have some of the most mission-oriented, talented IT professionals in all the Federal Government. And we have the team we need to be successful. I am particularly pleased with the start in July 2016 of our new CEDCaP Chief Security Engineer. He brings with him 20 years of background in the field of information security, a strong history of private sector experience, and a wealth of knowledge about what it takes to secure Federal information systems.

With hard work from our team and Congressional support, I am confident the Census Bureau can achieve its objectives. I look forward to discussing other aspects of our planning for the 2020 Census with you. I am grateful for this opportunity to testify before the Subcommittee, and I am pleased to answer any questions you may have.

Thank you.

Kevin B. Smith
Associate Director for Information Technology and
Chief Information Officer (ADITCIO)
US Census Bureau

Kevin Smith began working as the Associate Director for Information Technology and Chief Information Officer (ADITCIO) at the US Census Bureau in June of 2016. He serves as the principal advisor to the Director and Deputy Director on information resources and information systems management. Kevin will be leading the Census Bureau's information technology program to deliver "Cross-Bureau" business value by establishing common enterprise IT services in collaboration with all the survey and program areas.

Prior to joining the US Census Bureau, Kevin worked in the public sector for the United States Patent and Trademarks Office (USPTO) and the Internal Revenue Service (IRS). Kevin led the USPTO as the Deputy Chief Information Officer and the Chief Information Security Officer to become a more agile development and customer centric delivery organization through leading the cultural and technological transformation into a high performing and secure DevOps service provider. He also led major initiative across the USPTO with the business areas that required new technology solutions with the right amount of business process changes to achieve legislative requirements. As a federal contractor for the Internal Revenue Service (IRS), Kevin directed the development and implementation of an innovative strategy and planning system for infrastructure technology modernization that has corrected past problems that were been in place to more effectively modernize their technology infrastructure while balancing their financial, risk, and technology pressures. Outside the federal government in the private sector, Kevin has experience in technology from the consulting, research & development, sales, and operational perspectives in the Fortune 100/500 space where he helped to stabilize technology in Financial and Manufacturing organizations as well as develop 1st of their kind solutions to resolve new problems that were facing the Media & Entertainment, Broadcast, and Life Sciences industries as they transitioned into the digital age.

Kevin has a Bachelor of Science degree in Computer Engineering from the University of Florida.