COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

November 16, 2016

STATEMENT FOR THE RECORD

ROBERT KLOPP
DEPUTY COMMISSIONER OF SYSTEMS
CHIEF INFORMATION OFFICER
SOCIAL SECURITY ADMINISTRATION

Chairman Hurd and Ranking Member Kelly, thank you for inviting me to testify today to discuss cybersecurity at the Social Security Administration (SSA).

In this testimony I will provide you with an update that describes our progress and open issues related to the external audits of our cybersecurity program; I will provide you with an update related to other projects that have resulted from our own examination of our systems; and I will provide you with a status of our efforts to protect personal information.

I would like to suggest one issue on-the-record for consideration by the Committee. The Council of Inspectors General has established a measurement standard for compliance with the Federal Information Security Management Act (FISMA) Information Technology (IT) Security guidelines. Unfortunately, the standard has changed significantly each of the past three years and, as a result, one cannot judge progress against a standard set of criteria. In FY 2015, the Inspectors General (IGs) introduced a maturity model for Information Security Continuous Monitoring, which, as stated in the Office of Management and Budget's (OMB) Annual Report to Congress, led to a decrease in overall agencies scores. In FY 2016, the IGs introduced a second maturity model for Incident Response, which will likely lead to a further decrease in scoring due to the scoring methodology. The maturity model provides agencies with context for performing risk assessments and identifying the optimal maturity level that achieves cost-effective security based on their missions and risks. The IGs indicate that they plan to coordinate with the Department of Homeland Security (DHS), OMB, and other key stakeholders, and extend the maturity model to other security domains for IGs to utilize in their FY 2017 FISMA reviews. In the meantime, however, metrics for those domains without an established maturity model are mapped to Maturity Model Indicators. These indicators will act as a stepping-stone, allowing IGs to reach preliminary conclusions similar to those achievable with a fully developed model

We will continue to work with our Inspector General to address deficiencies across these areas.

To that end, the SSA cybersecurity team is recognized as one of the better teams in the federal government. As I describe in my testimony, we have made significant strides forward since our last visit before this Committee in May.

In our last hearing, some Members voiced concerns about a lack of leadership on cybersecurity at the agency. I appreciate this concern, but I also think we need to be careful about assuming that any security weakness is the result of bad management. If the fact that there are vulnerabilities in our IT infrastructure reflects a lack of leadership, then I accept the responsibility for the lack of leadership. If the criteria is that, if DHS finds anything wrong, this reflects a lack of leadership, then I accept the responsibility. But this also means that every agency that has a vulnerability, exploited or not, has a leadership issue – and that means every agency, not just SSA.

The cost of continuously deploying ever better cybersecurity is growing with the many threats from bad actors. The ability to protect legacy systems becomes more difficult as modern cyber defenses are not built to protect 30-year-old systems.

The SSA can shift funding from our IT budget for cyber, but soaking up any savings by spending it on cyber does not fund continuous improvement. It does not fund IT modernization. The idea that the SSA, or any agency, can do more in cyber while simultaneously rebuilding our IT infrastructure is no less a fantasy than the idea that the country can modernize any other infrastructure – our roads, our dams, our electric grid, our military – without an investment.

My testimony includes a request to modernize IT and to fund improvements in cyber defenses. Wishing for better IT from cost cutting will not help. Wishing for cost-cuts with no investment will not help. Passing legislation without providing funding is not enough.

In the remainder of this testimony, I will outline the issues and remediation undertaken by my cybersecurity staff since our last hearing.

OIG FISMA Audit

In 2015, the Office of the Inspector General (OIG) FISMA Audit identified several areas where the agency needed to improve our program.

In FY 2016, we made substantial improvements and progress in securing applications and managing vulnerabilities for the vast majority of our systems resources.

It was noted that we needed to improve our application of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) requirements for our remote locations: regional offices, program service centers, and Disability Determination Service systems. This is a significant undertaking.

During Fiscal Year (FY) 2016, we established a security assessment and authorization process that resulted in providing authority to operate (ATO) for 221 software applications in our regional offices and program service centers. This regional ATO process builds on our mature and robust RMF process for our centralized systems. We also improved our system inventory management process by expanding the use of an automated inventory software to capture details about applications housed remotely. We have not closed this issue but we are making significant progress.

We conducted a review of our national teleservice center system hosted by AT&T. After directing the vendor to make a series of changes, we granted an ATO. We conducted security reviews of other external contractor-operated systems using the same NIST processes we use for our internal systems. We include contractor systems in our automated inventory.

Auditors noted room to improve our access controls in order to prevent unauthorized access to our systems and data.

In FY 2016, we implemented an automated Security Access Management portal solution to replace our paper-based access request and approval process and established an authoritative database for contractor access. We implemented a Security Administration Reports Application and began the implementation of an automated Access Removal Tool for terminating or disabling logical and physical access for separated employees and/or contractors.

We expanded our user account review process to increase our focus on privileged user accounts and procured a new technical solution to further strengthen and automate management over our privileged user accounts.

We updated our security and privacy training to reflect the current threat landscape. Nearly 85,000 of our employees and contractors completed our annual training that covered a range of topics including protection of sensitive data, such as personally identifiable information, and how to prevent, detect, and report security incidents or suspected incidents when they occur. Additionally, we conducted ongoing training exercises to test our users' ability to detect social engineering attacks such as email phishing.

The auditor cited a weakness in tracking completion of security awareness training for all contractors.

We previously noted the establishment in FY 2016 of a contractor database. This database will log contractors' completion of mandatory security and privacy awareness training.

Audits suggested that we needed to continue improving our threat and vulnerability management process.

In FY 2016, we expanded our enterprise-wide penetration-testing program and implemented new tools to improve our detection of potential vulnerabilities across our network. This implementation has allowed us to find certain security threats in near real time.

The auditor cited a weakness that SSA had not implemented plans to close Information Security Continuous Monitoring skill gaps, knowledge, and required resources.

We began working with DHS under their Continuous-Monitoring-as-a-Service phase of the Continuous Diagnostics and Mitigation (CDM) program, which will allow us to feed information automatically about our asset, configuration and vulnerability posture directly to DHS to feed the federal dashboard, thereby improving visibility into all federal agencies. It also provides us with new capabilities to prevent unauthorized software on our network. While we have trained staff with the necessary skills and resources to meet all CDM program requirements, we face challenges similar to all Federal agencies in attracting and retaining cybersecurity talent.

DHS Cyber Exercises

We participated in several exercises where DHS staff were allowed access to our systems to find issues. There are several recommendations resulting from these exercises.

We have created a regimen that allows both DHS and our cyber staff to scan the mainframe environment regularly for vulnerabilities. Our regularly scheduled scans have found no significant issues there to date.

In addition, at our last hearing before HOGR it was pointed out that we needed to change the process where we notified OIG of a DHS exercise but waited for a formal request from them for the results, to a process where we automatically shared results after each exercise. We have done so.

FITARA Scorecard

In the May 2015 Federal Information Technology Acquisition Reform Act (FITARA) scorecard the agency received an overall grade of "C." Although we received high grades in some categories, we received "F"s in two categories.

We received an "F" for "Incremental Development." Our efforts to reduce time and increase the number of times we deliver product increments is paying off. In addition, we are actively pushing Agile development methods in order to improve further our ability to develop software faster and cheaper.

We also received an "F" for "Data Center Consolidation." Since our last hearing, we have finished the development and deployment of our Urbana data center. Recently, your staff toured the facility and, it is my understanding, they came away impressed. With the closure of this project, the agency is fully consolidated and runs only two data centers: a primary and a back-up. This should improve our grade to an "A," fully consolidated.

We believe that these two improvements would push our overall grade to a "B" if the criteria were to stay the same.

Internal Projects and Status

This topic provides an overview of capabilities-in-place and of other projects unrelated to external parties.

General Notes

The agency is incubating a series on modern IT capabilities in preparation for a series of funded IT modernization programs. Each of these new technologies goes through a comprehensive review before receiving an ATO.

Cloud Computing
We utilize the General Services Administration's Federal Risk and Authorization Management (FedRAMP) program to guide the security of our cloud-based systems. In FY 2016, we issued our first provisional cloud ATO for our Agency Cloud Infrastructure platform as a service.

Enterprise Data Warehouse

We are deploying new Open Source technologies as part of the first agency-wide decision support/ Enterprise Data Warehouse product. These technologies build upon the ATO for cloud computing and this new platform has received authorization to operate.

Identity Assurance for Public Facing Applications

The agency is planning to implement methods that adhere to the NIST Identity Assurance Level 3, when providing a citizen access to our online services.

This fall, the agency moved to improve our ability to authenticate users with existing IDs by implementing a technique called multi-factor authentication (MFA). Our implementation of Multi-factor authentication requires users to respond to a prompt sent to a device in their possession.

Unfortunately, our implementation created a security barrier that some citizens could not overcome so we backed out MFA and immediately began designing a new MFA approach that would implement secondary factors that allow any computer user to login. We expect this new protection to be deployed in the first half of calendar 2017.

Incident Response

We have a comprehensive Incident Response process in place. We prepare, plan and conduct Incident Response testing every six months. Our testing in FY 2016 included establishing a process to fund our recovery in the event of a large-scale breach. We also have an automated capability to report personally identifiable information losses and incidents detected by our Security Operations Center to DHS' United States Computer Emergency Readiness Team (US-CERT) within the required timeframes.

We perform a range of agency-wide activities designed to identify threats to our agency mission and operations, and plan for the recovery of IT assets needed to support our essential functions. We have established Continuity of Operations Plans (COOP) at the agency and component levels, which identify our mission essential functions. We have conducted a Business Impact Analysis to determine the potential adverse impact that the loss of our IT infrastructure would have on our ability to perform essential functions. We have further developed a Disaster Recovery plan that provides for full redundancy of our major systems. We conduct annual COOP testing and disaster recovery exercises that test the recovery of our major systems.

IT Modernization

I would like to emphasize that we also need to modernize our legacy systems to provide the modern infrastructure that incorporates modern cyber defenses. As we head into this period where a significant portion of our IT staff becomes eligible for retirement, we need to begin long-term efforts to modernize our infrastructure, our data architecture, and our software intellectual property. We need to accomplish this while we keep the current systems incrementally advancing and while we continue to expand our commitment to cybersecurity. The Administration's proposal for the IT Modernization Fund would provide an additional opportunity to secure much needed IT modernization funding.

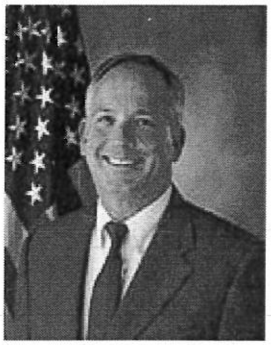
To that end, we need a sustained, long-term investment to make the changes needed to develop a fully modern IT infrastructure that is capable of supporting the immense responsibilities I described earlier in my testimony. That is why the President's Budget for FY 2017 requests multiyear funding of $300 million spread over four years, to undertake an IT modernization project that will bring our systems current. In FY 2017, $60 million is included as part of the FY 2017 President's Budget. The FY 2017 President's Budget also contains a mandatory proposal for additional IT modernization funding – $80 million each year in FYs 2018-2020. The project will require effort and long-term investment in several areas including modernization in computer languages, databases, and infrastructure.

We need this additional IT modernization funding because our annual funding levels have been insufficient to undertake this important IT work. We are working hard to manage the agency with far less money than we need. Our FY 2016 enacted budget was around $350 million less than the President's Budget request. As a result, we are seeing service degradation in many areas. SSA's core operating budget has shrunk by 10 percent since FY 2010 after adjusting for inflation, while the number of Social Security beneficiaries rose by 12 percent over the same period. We are greatly concerned about FY 2017, when we will serve a record number of beneficiaries, at a time when people are already facing longer wait times for service in our frontline offices.

Each year, over $300 million of our budget represents fixed cost growth for things such as increases in salaries, benefits, rent for our buildings, and guard costs. The continuing resolution (CR) leaves us with few resources to improve overall service. With services already in a fragile state, it is critical that we receive sufficient funding when Congress passes a full-year budget for FY 2017 – and it is critical to receive adequate funding to carry out IT modernization to protect the public's data and enhance service to the public. The FY 2017 President's Budget request of $13.067 billion is necessary to rebound from this year's constraints, to improve service to the public, to maintain service hours to the public in our offices, and to begin the needed work to protect and modernize our IT infrastructure. I would be happy to have our budget office brief you or your staff in greater detail.

Conclusion

Thank you for holding this hearing. I would be pleased to answer any questions you may have.



Robert Klopp
Chief Information Officer and
Deputy Commissioner for Systems

Rob Klopp is the Chief Information Officer (CIO) for the Social Security Administration. Rob started at the Agency as the Chief Technology Officer in January of 2015 and assumed the role of CIO and Deputy Commissioner of Systems the following August. Rob was recruited by the United States Digital Services team specifically to support the Agency.

He comes to Baltimore from the Silicon Valley where he has worked for both large software enterprises and for smaller start-ups. You may know of some of the start-ups. Greenplum, for example, was acquired by EMC and Teradata is now a leading company in the relational database and data warehouse markets. Rob spent nearly two years based in Switzerland as the EMC/Greenplum CTO for Europe, the Middle East, and Africa. He also worked in the consulting services space for EDS, now part of HP, and for what is now KPMG, as well as in his own boutique consultancy. He founded a little software start-up that was sold to a large database company. Rob started his career out of college in the Government arena with the State of California where he was a mainframe systems programmer.

Within these firms, Rob has filled both technical and executive roles; sometimes facing the engineering and product side of the business and sometimes facing the end-users, but always with both feet grounded in the technology.

Rob also publishes a popular blog on database technology: the Database Fog Blog and is a regular contributor to the blog at the CIO.gov site.