U.S. DEPARTMENT OF EDUCATION: INFORMATION SECURITY REVIEW

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

NOVEMBER 17, 2015

Serial No. 114–84

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

22–383 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
KATIE BAILEY, *Government Operations Subcommittee Staff Director*
MICHAEL FLYNN, *Counsel*
SHARON CASEY *Deputy Chief Clerk*

CONTENTS

U.S. DEPARTMENT OF EDUCATION: INFORMATION SECURITY REVIEW

Tuesday, November 17, 2015

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 10:01 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Jordan, Walberg, Amash, Gosar, Gowdy, Massie, Meadows, Mulvaney, Buck, Walker, Blum, Hice, Carter, Grothman, Hurd, Palmer, Maloney, Clay, Connolly, Kelly, DeSaulnier, and Lujan Grisham.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will come to order. Without objection, the chair is authorized to declare a recess at any time.

We appreciate you joining us for our review of the United States Department of Education: The Information Security Review.

And at this time I would like to yield to the gentleman from Texas, Mr. Hurd.

Mr. HURD. Thank you, Chairman Chaffetz.

Today's hearing is an opportunity, an opportunity to start managing the cybersecurity vulnerabilities and risks that this nation faces every day.

I said it during the July hearing this committee held on the data breach of the Office of Personnel Management. It is an undeniable fact that America is under constant attack. I am not talking today about bombs dropping or missiles launching, but the constant stream of cyber weapons aimed at our data.

The good news for this hearing, we are not talking about a data breach today. But, Dr. Harris, I want my message to be heard loud and clear. You do not want to be before this committee explaining to the American people how you left a PII of the sons and daughters of millions of Americans vulnerable to hackers.

And it is important to realize that this is not a problem without solutions. The GAO and the inspector general have made recommendations, not to mention the standards, policies, and programs of OMB, DHS, and NIST. What I am trying to tell you is that this is not an issue of technology. This is an issue of management and leadership.

Dr. Harris, you are on the spot today but don't think you are being singled out. I have put and we have put Federal CIOs and agency heads on notice time and again. Whether it be on FITARA implementation, data privacy, encryption, or compliance with Fed-

eral information security policies and practices, this committee will be watching. We are talking to the inspectors general and reading their recommendations. Federal CIOs and agency heads need to be implementing the recommendations of the IGs and GAO or be able to explain to me and this committee why they didn't.

Thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. I thank the gentleman. And I want to just kind of—let's stick to the facts here and go through some key numbers and metrics because the liability, the vulnerability is enormous.

Roughly 17 years ago the liability to the taxpayers in this category—we are talking about the Department of Education. Outstanding student loans 17 years ago was roughly $150 billion. Today, taxpayers are liable for roughly $1.18 trillion, making the Department of Education essentially the size of Citibank.

Most people don't realize how large and enormous of a financial institution the Department of Education is. There are roughly 40 million borrowers utilizing the Department of Education as essentially their bank and financial institution.

This is an organization, the Department of Education, that spends some $683 million—spent $683 million this year on information technology.

[Slide.]

Chairman CHAFFETZ. But as we put up this slide, doing a self-assessment, if we can do the FITARA self-assessment, this is also an organization based on their self-assessment gets an overall "F" grade as it relates to IT. So we can look at data center consolidation, IT portfolio review savings, incremental development, and risk assessment transparency, earning it an "F".

Chairman CHAFFETZ. You can take down that slide now.

This is a system that we are not necessarily—all the systems are utilizing encryption. This is a department where the OMB cyber sprint exercise—if you would put up the second slide.

[Slide.]

Chairman CHAFFETZ. OMB has engaged in the cyber sprint. It is one of, I believe, only four agencies in all of Federal Government where they scored a negative 14 percent, negative 14 percent. You can put down that slide. We can provide that information. It is very hard to read in that group.

Chairman CHAFFETZ. But one of four institutions where it actually scored negative on assessment of, say, dual authentication. In fact, the inspector general went in and looked at the Department of Education's IT operations, and the report finds "the department-wide information systems continue to be vulnerable to security threats." The inspector general made 16 findings, 6 of which are repeat findings. The inspector general made a total of 26 recommendations, 10 of which are repeat recommendations.

So how big is the vulnerability? We talked about it in terms of dollars. Americans need to know that the Department of Education holds roughly 139 million Social Security numbers in the Central Processing System. But let's also remember that 139 million Social Security numbers isn't necessarily all of them because it does not include all the systems. That is just the Central Processing System. It does not include information for parents who submitted informa-

tion but whose children did not get aid. If your child applies for aid, you are going to have perhaps your mother's information, perhaps your father's information in there as well. That is also in the system and potentially very vulnerable.

The Central Processing System processes Federal aid applications at roughly 22 million of them per year. We have been talking a lot about the vulnerability of the Office of Personnel Management, OPM, understanding the vulnerability where we believe it is 22 million. The vulnerability at the Department of Education, we are talking about a trillion dollars but we are also talking about over 130 million Americans.

The Department has 184 information systems, 184. This is just the Department of Education. One hundred and twenty are run by contractors, 29 are valued by OMB as high assets. But one of the concerns that we have here is that the inspector general also looked at what's called the COD, the Common Origination and Disbursement system. It is deemed as a major system. It is what is actually the system used to disburse Federal student aid to students and borrowers. This year alone there was roughly $109 billion in direct loans and $31 billion in Pells disbursed through the COD.

One of the fundamental problems that we have had here is access to that information and allowing the inspector general to be able to go in and peak at the system, test and verify it. But this is also a problem.

Another key system is the National Student Loan database, which houses significant borrower information. It is called the NSLDS, the National Student Loan database, has 97,000 accounts. This is the people that have access to student loans. These are the schools, the contractors. That is a lot of people being able to tap in and have access to this system.

But it is our understanding that only 5,000 of the 97,000 have actually undergone a background check, which again begs the question about allowing access to information that could be potentially vulnerable. It begs a lot of questions about safety, security, and integrity of this system.

We are also going to hear—and we have a hearing today on the Department of Education, but we also have hearings tomorrow on the Department of Education. And part of what we are going to hear tomorrow is that Department of Education was potentially responsible for roughly $4 billion in improper payments, $4 billion.

So we go home, we talk to our constituents about roads, bridges, infrastructure, about getting more money in the classroom. Utah has the lowest, lowest in the Nation. We are not proud of it, lowest spending per pupil in the Nation, and yet the Department of Education sends out $4 billion in improper payments. You know what a difference that would make in my classroom where we have got way too many kids in the classroom?

I am just telling you, it has become a monster, an absolute monster. We don't know who is in there. We don't know what they are doing. We know there are improper payments. And the inspector general, the person we trust the most to go in there and take a look at it can't even have access because there are so many contractors who say no, we are not going to let you look in there; no, you

can't see it. And that is a problem. That is a problem that has got to change.

Chairman CHAFFETZ. So I have gone well past my time. There is lots to talk about over the next 2 days. This is going to be a good, healthy hearing. I appreciate members' participation. There are a lot of competing hearings. You are going to see members coming and going as the second day back, 10:00 a.m., there are a lot of hearings going on. But this should be a good hearing.

And I now recognize the ranking member, Mr. Connolly, for his opening statement.

Mr. CONNOLLY. Thank you, Mr. Chairman. And thank you to our panelists for being with us today.

I appreciate the opportunity to examine the information technology and security programs and practices within the Department of Education and the Federal Student Aid program.

This department might not seem like an obvious target of cyber-related threats, but it is responsible for managing and securing student loan portfolios of more than $1 trillion, as you indicated, Mr. Chairman, along with the personal information of more than 50 million students between Federal loan borrowers, Pell Grant recipients, and other assistance programs. And as you indicated, Mr. Chairman, that may be the tip of the iceberg when one looks at over 130 million Social Security numbers available to the Department.

In the wake of two massive data breaches disclosed by the Office of Personnel Management earlier this year, which collectively put at risk the personal information of more than 28 million current and former Federal employees and their families, including Members of Congress like myself, every Federal agency ought to be reassessing its own information security protocols and reinforcing efforts to detect and deter cyber attacks and other threats.

Perhaps this should be the first of a recurring set of hearings to gauge successes and shortfalls across agencies when it comes to protecting the vast amount of sensitive information held by the Federal Government. I know Mr. Hurd and Mr. Meadows and yourself, Mr. Chairman, intend to do that certainly with the implementation of FITARA, but maybe we need to do it with cybersecurity as well.

I think we would find most agencies in a similar situation to this department, which has made some progress in fortifying its information security defenses in recent years but continues to struggle with recurring vulnerabilities.

In its latest report in the Department's efforts to implement the Federal Information Security Modernization Act, FISMA, the inspector general identified 16 findings with 26 recommendations, one-third of which are repeat recommendations, Dr. Harris. Last year's audit found that the Department did not perform adequate remediation of weaknesses identified in previous OIG audit reports. That is very troubling in light of the OPM breach.

While it appears the Department has beefed up its remediation efforts, there is still obviously much work to be done, and I am confident that unfortunately this is not the only department with these kinds of problems.

This year's audit flagged weaknesses across four key areas: continuous monitoring, configuration management, instant response and reporting, and remote access management. For example, the IG found user accounts from inside Federal employees and outside Federal contractors with excessive or unnecessary permissions and unauthorized access to data. In fact, one of the Department's IT service contractors could not verify to the IG's satisfaction that its other non-Federal customers did not have unauthorized access to the Department's data through a shared service, very troubling.

Even more troubling, the OIG said it was able not only to gain access to the Department's network through a simulated attack, but also it was able to launch other attacks on systems connected to the Department while going completely undetected.

Another critical finding in the IG's report that applies to the Department of Education, as well as other Federal agencies, is that existing information security protocols, if implemented and implemented consistently throughout the organization, could and should be effective. That is the good news.

Nowhere is this more important than in cybersecurity and privacy training for new employees. To be successful here, we must bring about a wholesale cultural revolution so that Federal agencies and the workforce understand the critical importance of cyber safety, including basic elements of what may be called cyber hygiene.

Along those same lines, we must hold agencies accountable for implementation of the bipartisan FITARA legislation on which we recently held a hearing and issued a preliminary scorecard for agency progress. The chairman has already noted that scorecard for this department. One of the key reforms of that legislation, which I was pleased to co-write with the former chairman of this committee, is enhancing CIO authorities to increase transparency and improve risk management to address all of these issues.

Unfortunately, the Department of Education received an "F" rating on this preliminary assessment based in large part on its self-reporting of few IT investments, delivering functionality, and their ability to produce savings. That is a snapshot in time, and we are hoping that it is a work in progress and that the next snapshot will show that progress. I look forward to hearing from Mr. Harris about the steps he is taking to address both FISMA and FITARA challenges.

The severity of recent data breaches in both public and private sectors in recent years underscores the urgency for Federal agencies and Congress to get serious about investing in IT solutions that better secure our data and taking actions that will be clear deterrents for would-be hackers. This is a challenge that has confounded both Democratic and Republican administrations.

The number of IT security incidents reported by Federal agencies increased by 1,121 percent from the reporting period in the last several years. Unfortunately, these attacks on our private industries and government simply reflect the new normal of the 21st century where nation states represent advanced and persistent threats against one another, constantly seeking to gain unauthorized access to sensitive and classified information on each other's people, intellectual property, and sensitive security information.

The likes of North Korea, China, Russia, and Iran are increasingly testing the waters and becoming emboldened by the lack of reprisal or effective deterrents.

The House earlier this year did pass two bills on a bipartisan basis to encourage voluntary sharing of information between the public and private sectors, but information-sharing is not enough. We need to get serious about strengthening our cyber workforce both within the Federal Government and among our private sector partners. We also need to devise more effective data breach notification policies so that victims are aware of the fact they may have been compromised.

As my colleagues know, it has now been almost 4 months since the breach on background records was announced, and notifications are still being made.

So, Mr. Chairman, I appreciate this opportunity to look at what the Department of Education is doing right and what it can improve upon with respect to securing data, but obviously, this can't be the only hearing. Successfully detecting, defending, and deterring cyber threats will take a concerted effort across all agencies and among our private partners. And I thank you, Mr. Chairman, because this hearing clearly sends a signal this committee will take that charge seriously.

I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We will hold the record open for 5 legislative days for any members who would like to submit a written statement.

And it is now my pleasure to recognize our witnesses. We are pleased to welcome Mr. Greg Wilshusen, who currently serves as the director of Information Security Issues at the Government Accountability Office where he leads cybersecurity- and privacy-related studies and audits of the Federal Government and critical infrastructure.

We also are joined by Ms. Kathleen Tighe, who serves as the inspector general of the United States Department of Education. Ms. Tighe also chairs the Council of Inspectors General on Integrity and Efficiency, and in 2011 was appointed by President Obama to the Recovery, Accountability, and Transparency Board and the Government Accountability and Transparency Board.

And we also are joined by Dr. Danny Harris, who currently serves as the chief information officer at the United States Department of Education. Prior to his tenure as CIO, Dr. Harris served as the chief financial officer at the Department of Education where he started his career as a computer analyst.

We welcome you all.

Pursuant to committee rules, witnesses are to be sworn before they testify, so if you will please rise and raise your right hand.

[Witnesses sworn.]

Chairman CHAFFETZ. Thank you. Please be seated, and let the record reflect that the witnesses all answered in the affirmative.

We would like some time to be set aside for some robust discussion, so we would appreciate it if you would limit your testimony to 5 minutes. And obviously your entire written statement will be made part of the record.

We will start with Mr. Wilshusen, and he is now recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF GREG WILSHUSEN

Mr. WILSHUSEN. Chairman Chaffetz, Ranking Member Connolly, and members of the committee, thank you for the opportunity to testify at today's hearing on information security at the Department of Education.

As requested, my statement will address information security of Federal agencies, including Education.

Before I begin, if I may, I would like to recognize several members of my team who were instrumental in developing my statement and performing the work underpinning it. Larry Crosland, Assistant Director; and Rosanna Guerrero led this body of work. Lee McCracken and Christopher Businsky also made significant contributions.

Mr. Chairman, for 18 years GAO has designated Federal information security to be a government-wide high-risk area. In February we expanded this area to include protecting the privacy of personally identifiable information. Recent security incidents such as the OPM data breaches underscore the vulnerability of Federal systems and highlight the evolving and sophisticated nature of the cyber threats that confront Federal security personnel on a daily basis.

Over the last several years, Federal agencies have reported a sharp increase in the number of information security incidents, which have risen from about 5,500 in fiscal year 2006 to over 67,000 in fiscal year 2014, an increase of approximately 1,100 percent. Similarly, the number of incidents involving personally identifiable information has more than doubled since fiscal year 2009 to over 27,000 in fiscal year 2014.

Given the risks posed by cyber threats and the increasing number of incidents, it is crucial that Federal agencies take appropriate steps to secure their systems and information. However, we and agency inspectors general have continued to identify significant deficiencies in controls protecting Federal information systems. For example, 19 of the 24 agencies covered by the Chief Financial Officers Act reported a significant deficiency or material weakness in information security for financial reporting purposes in fiscal year 2014. For its part, the Department of Education reported a significant deficiency which is less severe than a material weakness but important enough to merit attention by those charged with governance.

As we previously reported for fiscal year 2014, nearly each of the 24 agencies, including Education, reported weaknesses in most of the five general control categories that we track. Like 21 other agencies, Education had weaknesses reported in controls that are intended to prevent, limit, and detect unauthorized or inappropriate access to computer networks and sensitive information.

Similar to most agencies, Education also had weaknesses reported in its configuration management of its computing system, continuity of operation controls, and management of its information

security program. On the plus side, unlike 15 other agencies, Education did not have weaknesses reported in its controls to segregate incompatible duties to—among different individuals.

For deficiencies in security controls and the efforts required to mitigate them, inspectors general at 23 of the 24 agencies, including Education, declared information security as a major management challenge for their agency in fiscal year 2014.

Over the past 6 years, GAO has made about 2,000 recommendations aimed at improving their information security programs and controls. To date, agencies have implemented about 58 percent of them.

Recent actions initiated by the Federal chief information officer such as the 30-day Cybersecurity Sprint and issuance of a Cybersecurity Strategy and Implementation Plan indicate a new level of attention by OMB to the security of Federal networks, systems, and data at civilian agencies. Effective and timely implementation of this strategy and the rest of GAO's recommendations, as well as those made by agency IGs, will bolster agencies' ability to protect their information systems and information.

Mr. Chairman, Ranking Member Connolly, members of the committee, this concludes my opening statement. I'd be happy to answer your questions.

[Prepared statement of Mr. Wilshusen follows:]

GAO Highlights

Highlights of GAO-16-228T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

The federal government faces an evolving array of cyber-based threats to its systems and data, and data breaches at federal agencies have compromised sensitive personal information, affecting millions of people. Education, in carrying out its mission of serving America's students, relies extensively on IT systems that collect and process a large amount of sensitive information. Accordingly, it is important for federal agencies such as Education to implement information security programs that can help protect systems and networks. GAO has identified federal information security as a government-wide high-risk area since 1997, and in February 2015 expanded this to include protecting the privacy of personally identifiable information.

This statement provides information on cyber threats facing federal systems and information security weaknesses identified at federal agencies, including Education. In preparing this statement, GAO relied on previously published work and updated data on security incidents and federal cybersecurity efforts.

What GAO Recommends

Over the past 6 years, GAO has made about 2,000 recommendations to federal agencies to correct weaknesses and fully implement agency-wide information security programs. Agencies have implemented about 58 percent of these recommendations. Agency inspectors general have also made a multitude of recommendations to assist their agencies.

View GAO-16-228T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

November 17, 2015

INFORMATION SECURITY

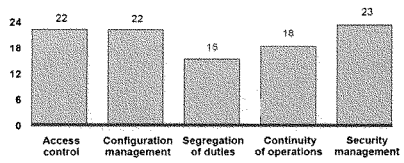
Department of Education and Other Federal Agencies Need to Better Implement Controls

What GAO Found

Cyber-based risks to federal systems and information can come from unintentional threats, such as natural disasters, software coding errors, and poorly trained or careless employees, or intentional threats, such as disgruntled insiders, hackers, or hostile nations. These threat sources may exploit vulnerabilities in agencies' systems and networks to steal or disclose sensitive information, among other things. Since fiscal year 2006, the number of reported information security incidents affecting federal systems has steadily increased, rising from about 5,500 in fiscal year 2006 to almost 67,200 in fiscal year 2014. At the Department of Education, the number of incidents reported since 2009 has fluctuated, but generally increased.

GAO reported in September 2015, that most of 24 major agencies (including Education) had weaknesses in at least three of five major categories of information security controls for fiscal year 2014. These are controls intended to (1) limit unauthorized access to agency systems and information; (2) ensure that software and hardware are authorized, updated, monitored, and securely configured; (3) appropriately divide duties so that no single person can control all aspects of a computer-related operation; (4) establish plans for continuing information system operations in the event of a disaster, and (5) provide a security management framework for understanding risks and ensuring that controls are selected, implemented, and operating as intended. The figure below shows the number of agencies with weaknesses in these control categories.

Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014



Source: GAO analysis of agency, inspector general, and GAO reports as of May 2015. | GAO-16-228T

In addition, 19 agencies—including Education—reported that information security control deficiencies were either a material weakness or a significant deficiency for fiscal year 2014. Further, inspectors general for 23 of 24 agencies, including Education, cited information security as a major management challenge. In prior reports, GAO and inspectors general have made thousands of recommendations to agencies to address deficiencies in their information security controls and weaknesses in their programs, but many of these recommendations remain open. Until agencies implement these recommendations, sensitive information will remain at risk of unauthorized disclosure, modification, or destruction.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Thank you for the opportunity to testify at today's hearing on information security at the Department of Education (Education). As requested, my statement today will address cyber threats facing federal systems and information and security control weaknesses that have been identified at federal agencies, including Education.

As you know, the federal government faces an evolving array of cyber-based threats to its systems and data, as illustrated by recently reported data breaches at federal agencies, which have affected millions of current and former federal employees, and the increasing number of incidents reported by agencies. Such incidents underscore the urgent need for effective implementation of information security controls at federal agencies.

Since 1997, we have designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Most recently, in the February 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)[1]—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities.[2]

In preparing this statement, we relied on our previous work addressing cyber threats and federal information security efforts. We also relied on the number of incidents previously reported by Education; information technology spending previously reported by the Office of Management and Budget (OMB) and federal agencies; and recently reported data from

[1]Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

[2]See GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

the Cybersecurity Sprint.[3] The prior reports cited throughout this statement contain detailed discussions of the scope of the work and the methodology used to carry it out.

All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A list of related GAO products is provided in attachment I.

Background

As computer technology has advanced, the federal government has become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Federal agencies rely on computer systems to transmit proprietary and other sensitive information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services.

Ineffective protection of these information systems and networks can impair delivery of vital services, and result in

- loss or theft of computer resources, assets, and funds;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as personally identifiable information;
- disruption of essential operations supporting critical infrastructure, national defense, or emergency services;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in government;
- use of computer resources for unauthorized purposes or to launch attacks on other systems;
- damage to networks and equipment; and

[3]In June 2015, the Federal Chief Information Officer launched the 30-day Cybersecurity Sprint, during which agencies were to take immediate actions to combat cyber threats within 30 days. Actions included patching critical vulnerabilities, tightening policies and practices for privileged users, and accelerating the implementation of multifactor or strong authentication.

- high costs for remediation.

Recognizing the importance of these issues, Congress enacted laws intended to improve the protection of federal information and systems. These laws include the Federal Information Security Modernization Act of 2014 (FISMA 2014),[4] which, among other things, reiterated the 2002 FISMA requirement for the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information or information systems. This includes protections for information collected or maintained on behalf of the agency and information systems used or operated by a contractor of an agency or other organization on behalf of an agency.

In addition, the act continues the requirement for federal agencies to develop, document, and implement an agency-wide information security program. The program is to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other organization on behalf of an agency.

The act also authorizes the Department of Homeland Security (DHS) to (1) assist the Office of Management and Budget (OMB) with overseeing and monitoring agencies' implementation of security requirements; (2) operate the federal information security incident center; and (3) provide agencies with operational and technical assistance, such as that for continuously diagnosing and mitigating cyber threats and vulnerabilities.

Department of Education Relies on Information Technology Systems Containing Sensitive Information

The mission of the Department of Education is to serve America's students and promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access. In carrying out its mission, the department is responsible for four major types of activities:

- establishing policies relating to federal financial aid for education, administering distribution of those funds, and monitoring their use;

[4]The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) (2014 FISMA) largely superseded the very similar Federal Information Security Management Act of 2002 (Title III, Pub. L. No. 107-347, Dec. 17, 2002) (2002 FISMA).

- collecting data and overseeing research on America's schools and disseminating this information to Congress, educators, and the general public;
- identifying the major issues and problems in education and focusing national attention on them; and
- enforcing federal statutes that prohibit discrimination in programs and activities receiving federal funds and ensuring equal access to education for every individual.

To support these activities, the department relies on a variety of information technology (IT) systems and infrastructure. Moreover, the department's systems contain large volumes of sensitive information such as personnel records, financial information, and personally identifiable information. According to a fiscal year 2015 inspector general report, about 70 million users, which included students and borrowers, utilized the systems supporting the department's federal student aid program.[5]

Cyber Threats to Federal Systems Continue to Evolve amid Increasing Numbers of Incidents

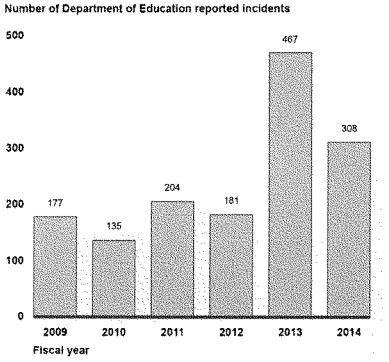
Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, software coding errors, and the actions of careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees and other organizational insiders, foreign nations engaged in espionage and information warfare, and terrorists.

These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary or personal gain or pursuing a political, economic, or military advantage. For example, insiders can pose threats because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system, steal system data, or disclose sensitive information without authorization. The insider threat includes inappropriate actions by contractors hired by the organization, as well as careless or poorly trained employees.

[5]Department of Education, Office of Inspector General, *The U.S. Department of Education's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014*, Report No. ED-OIG/A11O0001 (Washington, D.C.: November 2014).

As we reported in February 2015,[6] since fiscal year 2006, the number of information security incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT)[7] affecting systems supporting the federal government has steadily increased each year. Specifically, the number of reported incidents rose from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent. At Education, the number of reported incidents has fluctuated during the period from fiscal year 2009 to fiscal year 2014, with the department reporting 308 incidents in fiscal year 2014 after reaching a high of 467 in fiscal year 2013.

Figure 1: Information Security Incidents Reported to the U.S. Computer Emergency Readiness Team by the Department of Education, Fiscal Years 2009 through 2014



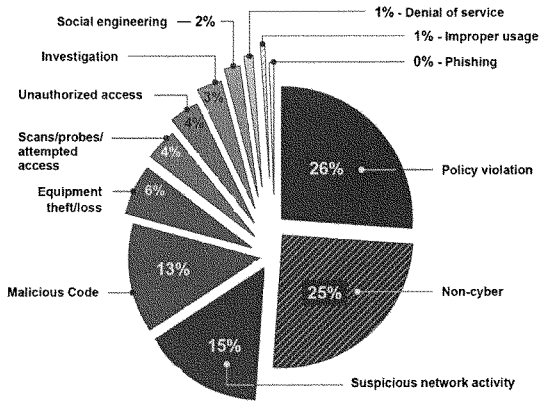
Source: GAO analysis of United States Computer Emergency Readiness Team data for Education for fiscal years 2009 to 2014. | GAO-16-228T

Figure 2 shows the different types of incidents reported by Education in fiscal year 2014.

[6]GAO-15-290.

[7]When incidents occur, agencies are to notify US-CERT.

Figure 2: Fiscal Year 2014 Information Security Incidents by Type as Reported by the Department of Education



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-16-228T

The types of incidents reported by Education are generally consistent with those reported by the other 23 major federal agencies, with a few exceptions. For example, at 26 percent, policy violations constituted the highest percentage of incidents reported by Education for fiscal year 2014. Policy violations involve incidents of mishandling data in storage or transit, such as digital PII records. In contrast, only 17 percent of incidents reported by the 24 major federal agencies were policy violations. The second highest percentage of incidents reported by Education was non-cyber incidents, at 25 percent, which was the same percentage reported by federal agencies. Non-cyber incidents are those that include PII spillages or possible mishandling of PII which involve hard copies or printed material as opposed to digital records.

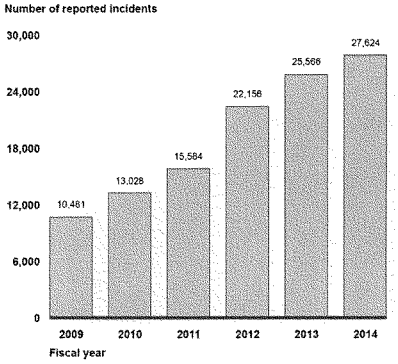
Suspicious network activity, at 15 percent, and malicious code, at 13 percent, were the third and fourth highest percentages of incidents that Education reported for fiscal year 2014. Suspicious network activity refers to incidents identified through Einstein[8] data analyzed by US-CERT, and malicious code incidents are successful executions or installations of malicious software which are not immediately quarantined and cleaned by preventative measures such as antivirus tools. Suspicious network activity made up 3 percent of the 24 major federal agencies' reported incidents, and malicious code constituted 11 percent of the incidents federal agencies reported for fiscal year 2014.

Finally, only 4 percent of the incidents reported by Education were for scans/probes/attempted access, which was the most widely reported type of incident by federal agencies (excluding non-cyber incidents). This type of incident can involve identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit.

Furthermore, the number of reported security incidents involving PII at federal agencies has more than doubled in recent years—from 10,481 incidents in fiscal year 2009 to 27,624 incidents in fiscal year 2014. (See fig 3.)

[8]Einstein is a system of systems that is intended to deliver a range of capabilities including intrusion detection and prevention, analytics, and information sharing. The goal of Einstein is to provide the federal government with an early warning system, improved situational awareness of intrusion threats, near real-time identification, and prevention of malicious cyber activity.

Figure 3: Incidents Involving Personally Identifiable Information Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies for Fiscal Years 2009 through 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2009-2014. | GAO-16-228T

These incidents and others like them can adversely affect national security and lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Examples at other agencies highlight the impact of such incidents:

- In June 2015, the Office of Personnel Management (OPM) reported that an intrusion into its systems affected the personnel records of about 4.2 million current and former federal employees. The Director stated that a separate but related incident involved the agency's background investigation systems and compromised background investigation files for 21.5 million individuals.
- In June 2015, the Commissioner of the Internal Revenue Service testified that unauthorized third parties had gained access to taxpayer information from its "Get Transcript" application. According to officials, criminals used taxpayer-specific data acquired from non-department sources to gain unauthorized access to information on approximately 100,000 tax accounts. This data included Social Security information, dates of birth, and street addresses. In an August 2015 update, the

agency reported this number to be about 114,000 and that an additional 220,000 accounts had been inappropriately accessed, which brings the total to about 330,000 accounts.

- In April 2015, the Department of Veterans Affairs' Office of Inspector General reported that two contractors had improperly accessed the agency's network from foreign countries using personally owned equipment.[9]
- In February 2015, the Director of National Intelligence stated that unauthorized computer intrusions were detected in 2014 on the networks of the Office of Personnel Management and two of its contractors. The two contractors were involved in processing sensitive PII related to national security clearances for federal employees.[10]
- In September 2014, a cyber intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 of its employees.[11]
- In October 2013, a wide-scale cybersecurity breach involving a U.S. Food and Drug Administration system occurred that exposed the PII of 14,000 user accounts.[12]

[9]Department of Veterans Affairs, Office of Inspector General, *Administrative Investigation Improper Access to the VA Network by VA Contractors from Foreign Countries Office of Information and Technology Austin, TX*, Report No. 13-01730-159 (Washington, D.C.: April 2015).

[10]James R. Clapper, Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, testimony before the Senate Committee on Armed Services (February 26, 2015).

[11]Randy S. Miskanic, Secure Digital Solutions Vice President of the United States Postal Service, *Examining Data Security at the United States Postal Service*, testimony before the Subcommittee on Federal Workforce, U.S. Postal Service and the Census, 113th Congress (November 19, 2014).

[12]Department of Health and Human Services, Office of Inspector General, *Penetration Test of the Food and Drug Administration's Computer Network*, Report No. A-18-13-30331 (Washington, D.C.: October 2014).

Similar to Other Agencies, Information Security Weaknesses Place Education's Systems and Sensitive Data at Risk

Given the risks posed by cyber threats and the increasing number of incidents, it is crucial that federal agencies, such as Education, take appropriate steps to secure their systems and information. We and agency inspectors general have identified numerous weaknesses in protecting federal information systems and information. Agencies, including Education, continue to have shortcomings in assessing risks, developing and implementing security controls, and monitoring results.

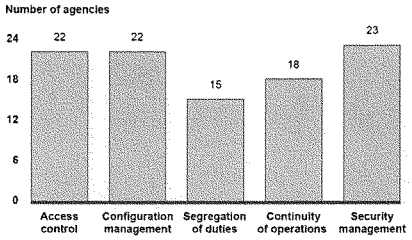
As we reported in September 2015, for fiscal year 2014 most of the 24 agencies covered by the Chief Financial Officers Act,[13] including Education, had weaknesses in most of the five major categories of information system controls.[14] These control categories are: (1) access controls, which limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure; (2) configuration management controls, intended to prevent unauthorized changes to information system resources (for example, software programs and hardware configurations) and assure that software is current and known vulnerabilities are patched; (3) segregation of duties, which prevents a single individual from controlling all critical stages of a process by splitting responsibilities between two or more organizational groups; (4) contingency planning,[15] which helps avoid significant disruptions in computer-dependent operations; and (5) agency-wide security management, which provides a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended. (See fig. 4.)

[13]The 24 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[14]GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO-15-714 (Washington, D.C.: Sept. 29, 2015).

[15]Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations.

Figure 4: Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014



Source: GAO analysis of agency, inspector general, and GAO reports as of May 2015. | GAO-16-228T

- **Access controls:** For fiscal year 2014, Education and 21 other agencies had weaknesses in electronic and physical controls to limit, prevent, or detect inappropriate access to computer resources (data, equipment, and facilities), thereby increasing their risk of unauthorized use, modification, disclosure, and loss. Specifically, Education's inspector general reported weaknesses in several key access control elements, including protecting the boundaries of its information systems and handling incidents. For example, the department did not implement controls to verify the security of non-government furnished equipment connecting to its network via virtual private client programs prior to authentication.

- **Configuration management:** For fiscal year 2014, 22 agencies, including Education, had weaknesses reported in controls that are intended to ensure that only authorized and fully tested software is placed in operation, software and hardware is updated, information systems are monitored, patches are applied to these systems to protect against known vulnerabilities, and emergency changes are documented and approved. For example, the department's configuration management guidance had not been updated since 2005 and its IT security baseline configuration guidance had not been updated since 2009.

- **Segregation of duties:** Fifteen agencies had weaknesses reported in controls for segregation of duties, although Education was not one of

them. These controls are the policies, procedures, and organizational structure that help to ensure that one individual cannot independently control all key aspects of a computer-related operation and thereby take unauthorized actions or gain unauthorized access to assets or records.

- **Continuity of operations:** Education and 17 other agencies had weaknesses reported in controls for their continuity of operations practices for fiscal year 2014. For example, Education did not consistently document the IT recovery procedures for its systems in accordance with National Institute of Standards and Technology (NIST) guidelines and departmental policies. In addition, the department did not consistently perform and document testing of contingency plans for certain systems.

- **Security management:** For fiscal year 2014, 23 agencies, including Education, had weaknesses reported in security management, which is an underlying cause for information security control deficiencies identified at federal agencies. An agency-wide security program, as required by FISMA, provides a framework for assessing and managing risk, including developing and implementing security policies and procedures, conducting security awareness training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. FISMA also requires agencies to develop and document an inventory of major systems. Regarding Education, the inspector general reported weaknesses in several key elements, including developing, documenting, and updating an inventory of its systems; periodically assessing risks to its systems; ensuring staff receive security awareness training; and remediating information security weaknesses. For example, the department did not implement corrective actions in a timely manner including 15 corrective actions that were completed late without a revised planned completion date.

In addition, independent reviews at the 24 agencies continued to highlight deficiencies in their implementation of information security policies and procedures. Specifically, for fiscal year 2014, 19 agencies—including Education—reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls

over their financial reporting.[16] Education was 1 of 12 agencies that reported that such weaknesses constituted a significant deficiency—which is less severe than a material weakness but important enough to merit attention by those charged with governance. Further, 23 of 24 inspectors general for the agencies, including Education, cited information security as a "major management challenge" for their agency.

In accordance with their responsibilities under FISMA, inspectors general at the 24 agencies continued to report on their respective agencies' fiscal year 2014 implementation of information security programs for these 11 program components:[17]

- **Risk management:** Inspectors general reported that program components for addressing risks at 17 agencies, including Education, were established. However, Education's inspector general identified exceptions. For example, the department's risk management program was not fully implemented and the process for system authorization needed improvement.
- **Configuration management:** Sixteen agencies, including Education, had established elements of their programs for managing changes to hardware and software. Education's inspector general noted exceptions in the department's configuration management policies, procedures, and plans and reported that they did not always comply with NIST and departmental guidance.
- **Incident response and reporting:** Twenty-one agencies, including Education, had established a program for detecting, reporting, and responding to security incidents. The Education inspector general noted that improvements were needed in the department's reporting

[16]A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, in internal control that is less severe than a material weakness, but important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[17]According to OMB, one inspector general did not report on its agency's contingency planning, contractor systems, and security capital planning programs for fiscal year 2014. Therefore, the results of only 23 agencies were included for these areas.

of incidents to the US-CERT and law enforcement agencies. For example, the inspector general reported that 4 of 45 sampled incidents were not reported to the US-CERT, as required.

- **Security training:** Along with 19 other agencies, Education had established a program for providing security training to staff.
- **Remedial actions:** Education and 18 other agencies had established program components for addressing deficiencies in information security policies, procedures, and practices.
- **Remote access:** Twenty-one agencies, including Education, had established program components for managing remote access to their networks. However, Education's inspector general also reported exceptions with this component. For example, the department lacked restrictions for virtual private network client programs on non-government-furnished equipment. In addition, it had not fully implemented two-factor authentication, and improvements were needed in the use of mobile devices when accessing the department's network.
- **Identity and access management:** Education, along with 15 other agencies, established program components for ensuring that users were properly identified and authenticated when accessing agency resources. However, Education's inspector general reported that the department needed to improve its password authentication process and had not fully implemented logical access controls.
- **Continuous monitoring:** Nineteen agencies, including Education, had established program components for continuously monitoring the effectiveness of security policies, procedures, and practices.
- **Contingency planning:** Education and 16 other agencies had established program components for ensuring continuity of operations for information systems in the event of a disaster or other unforeseen disruptions. However, Education's inspector general reported that the department's contingency plans were not always complete, and the process for testing the plans needed improvements.
- **Contractor systems:** At 17 agencies, including Education, inspectors general reported that program components for monitoring contractor systems had been established.

- **Security capital planning:** Education, along with 18 other agencies, had established program components for capital planning and investment for information security.

As we noted in our September 2015 report on federal information security, the annual FISMA reporting guidance that OMB and DHS provided to inspectors general was not complete, resulting in different interpretations among the inspectors general and inconsistent reporting results.[18] As a result, responses from inspectors general may not always be comparable or provide a clear government-wide picture of agencies' security implementation.

Accordingly, we recommended that OMB, in consultation with DHS and other stakeholders, enhance the reporting guidance so that ratings would be consistent and comparable across agencies. OMB generally concurred with our recommendation and stated that it would continue to work with DHS and other stakeholders to refine the FISMA reporting metrics and enhance reporting guidance.

Over the last several years, we and agency inspectors general have made thousands of recommendations to agencies aimed at improving their implementation of information security controls. For example, we have made about 2,000 recommendations over the last 6 years. Agency inspectors general have also made a multitude of recommendations to assist their agencies. Many agencies continue to have weaknesses in implementing these controls in part because many of these recommendations remain unimplemented. For example, agencies have not yet implemented about 42 percent of the recommendations we have made during the last 6 years. Until federal agencies take actions to implement the recommendations made by us and the inspectors general—federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats.

Federal Efforts Are Intended to Improve Cybersecurity

Although weaknesses continue to exist, the federal government has initiated or continued several efforts to protect federal information and information systems. The White House, OMB, and federal agencies have

[18]GAO-15-714.

launched several government-wide initiatives that are intended to enhance information security at federal agencies. These key efforts include the following.

Cybersecurity Cross-Agency Priority (CAP) Goals. Initiated in 2012, CAP goals are an effort to focus agencies' cybersecurity activity on the most effective controls. Education reported the following levels of performance with respect to metrics related to the CAP goals:

- **Trusted Internet Connections (TIC):** Aims to improve the federal government's security posture through the consolidation of external telecommunication connections by establishing a set of baseline security capabilities through enhanced monitoring and situational awareness of all external network connections. OMB established a 100 percent target for implementing TIC capabilities for fiscal year 2014 and reported that the 24 agencies covered by the Chief Financial Officers Act achieved an overall implementation rate of 92 percent. For fiscal year 2014, Education reported a 95 percent implementation rate.

- **Continuous Monitoring of Federal Information Systems:** Intended to provide near real-time security status and remediation, increasing visibility into system operations and helping security personnel make risk management decisions based on increased situational awareness. OMB established a fiscal year 2014 target of 95 percent and reported that overall the 24 agencies had achieved 92 percent implementation. Education reported 98 percent continuous monitoring of its assets at the end of fiscal year 2014.

- **Strong Authentication:** Intended to increase the use of federal smartcard credentials, such as personal identity verification and common access cards that provide multifactor authentication and digital signature and encryption capabilities. Strong authentication can provide a higher level of assurance when authorizing users' access to federal information systems. For fiscal year 2014, OMB established a 75 percent implementation rate, but indicated that the 24 agencies had implemented strong authentication for a combined 72 percent of their users. Education reported an 85 percent implementation rate at the end of fiscal year 2014.

The 30-Day Cybersecurity Sprint. In June 2015, in response to the OPM security breaches and to improve federal cybersecurity and protect systems against evolving threats, the Federal Chief Information Officer launched the 30-day Cybersecurity Sprint and instructed agencies to

immediately take a number of steps to further protect federal information and to improve the resilience of federal networks. One step was to accelerate the implementation of multi-factor authentication, such as the use of personal identity verification cards to gain access to federal networks, systems, and data. According to a report by the Executive Office of the President, the percentage of Education's users who used strong authentication decreased to 57 percent, one of only four agencies to show a decrease following the sprint.[19]

Agency Spending on Cybersecurity Activities. According to OMB, the 24 agencies covered by the Chief Financial Officers Act reported spending about $12.7 billion on cybersecurity activities in fiscal year 2014.[20] Of this amount, the 23 civilian agencies[21] reportedly spent about $3.75 billion or about 9 percent of the amount the agencies reportedly spent on information technology in fiscal year 2014.[22] For fiscal year 2014, Education reportedly spent about $32 million on cybersecurity, or roughly 5 percent of the amount it reportedly spent on information technology.[23] The agencies reported spending amounts for three major categories of cybersecurity activities: preventing malicious cyber activity; detecting, analyzing, and mitigating intrusions; and shaping the

[19]Executive Office of the President of the United States, *Cybersecurity Sprint Results* (Washington, D.C.: July 2015).

[20]OMB, *Annual Report to Congress: Federal Information Security Management Act*, (Washington, D.C.: Feb. 27, 2015).

[21]We excluded the Department of Defense from this analysis because the amount it reportedly spent on cybersecurity activities dwarfed the combined amount spent by the other 23 agencies and its inclusion would inappropriately skew the results.

[22]The 9 percent amount was computed by dividing $3.75 billion the 23 civilian agencies spent on cybersecurity activities by the amount they reportedly spent on information technology in fiscal year 2014, which according to the IT Dashboard was about $43.9 billion.

[23]The 5 percent amount was computed by dividing the $32 million spent on cybersecurity activities according to OMB by the amount spent on information technology (about $630 million according to the IT Dashboard).

cybersecurity environment.[24] Of the about $32 million it reportedly spent on cybersecurity activities, Education spent 34 percent on preventing malicious activity; 63 percent on detecting, analyzing, and mitigating intrusions; and 3 percent on shaping the cybersecurity environment.

In conclusion, the dangers posed by a wide array of cyber threats facing the nation are heightened by weaknesses in the federal government's approach to protecting its systems and information. While federal agencies, including the Department of Education, have established information security programs, weaknesses in these programs persist, and more needs to be done to fully implement them and to address existing weaknesses. In particular, implementing outstanding inspector general and GAO recommendations will strengthen agencies' ability to protect their systems and information, reducing the risk of a potentially devastating cyber attack.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my statement. I would be happy to answer your questions.

Contact and Acknowledgments

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other staff members who contributed to this statement include Larry Crosland, Assistant Director; Christopher Businsky; Rosanna Guerrero; Fatima Jahan; and Lee McCracken.

[24] **Preventing malicious cyber activity** is an area of spending that pertains to monitoring federal government systems and networks and protecting the data within from both external and internal threats. **Detecting, analyzing, and mitigating intrusions** is an area of spending on systems and processes used to detect security incidents, analyze the threat, and attempt to mitigate possible vulnerabilities. **Shaping the cybersecurity environment** is an area of spending on improving the efficacy of current and future information security efforts, such as building a strong information security workforce and supporting broader IT security efforts.

Attachment I: Related GAO Products

Critical Infrastructure Protection: Cybersecurity of the Nation's Electricity Grid Requires Continued Attention, GAO-16-174T. Washington, D.C.: October 21, 2015.

Maritime Critical Infrastructure Protection: DHS Needs to Enhance Efforts to Address Port Cybersecurity, GAO-16-116T. Washington, D.C.: October 8, 2015.

Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs, GAO-15-714. Washington, D.C.: September 29, 2015.

Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies. GAO-15-758T. Washington, D.C.: July 8, 2015.

Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies. GAO-15-725T. Washington, D.C.: June 24, 2015.

Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems. GAO-15-573T. Washington, D.C.: April 22, 2015.

Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data. GAO-15-337. Washington, D.C.: March 19, 2015.

Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems. GAO-15-221. Washington, D.C.: January 29, 2015.

Information Security: Additional Actions Needed to Address Vulnerabilities That Put VA Data at Risk. GAO-15-220T. Washington, D.C.: November 18, 2014.

Information Security: VA Needs to Address Identified Vulnerabilities. GAO-15-117. Washington, D.C.: November 13, 2014.

Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems. GAO-15-6. Washington, D.C.: December 12, 2014.

Consumer Financial Protection Bureau: Some Privacy and Security Procedures for Data Collections Should Continue Being Enhanced. GAO-14-758. Washington, D.C.: September 22, 2014.

Healthcare.Gov: Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses. GAO-14-871T. Washington, D.C.: September 18, 2014.

Healthcare.Gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls. GAO-14-730. Washington, D.C.: September 16, 2014.

Information Security: Agencies Need to Improve Oversight of Contractor Controls. GAO-14-612. Washington, D.C.: August 8, 2014.

Information Security: FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain. GAO-14-674. Washington, D.C.: July 17, 2014.

Information Security: Additional Oversight Needed to Improve Programs at Small Agencies. GAO-14-344. Washington, D.C.: June 25, 2014.

Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity. GAO-14-459. . Washington, D.C.: June 5, 2014.

Information Security: Agencies Need to Improve Cyber Incident Response Practices. GAO-14-354. . Washington, D.C.: April 30, 2014.

Information Security: SEC Needs to Improve Controls over Financial Systems and Data. GAO-14-419. Washington, D.C.: April 17, 2014.

Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk. GAO-14-405. Washington, D.C.: April 8, 2014.

Information Security: Federal Agencies Need to Enhance Responses to Data Breaches. GAO-14-487T. Washington, D.C.: April 2, 2014.

Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Model. GAO-14-464T. Washington, D.C.: March 26, 2014.

Information Security: VA Needs to Address Long-Standing Challenges. GAO-14-469T. Washington, D.C.: March 25, 2014.

Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology. GAO-14-125. Washington, D.C.: January 28, 2014.

Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation. GAO-14-44. Washington, D.C.: January 13, 2014.

Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent. GAO-14-34. Washington, D.C.: December 9, 2013.

Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness. GAO-13-776. Washington, D.C.: September 26, 2013.

Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts. Washington, D.C.: GAO-13-275. April 10, 2013.

Information Security: IRS Has Improved Controls but Needs to Resolve Weaknesses. GAO-13-350. Washington, D.C.: March 15, 2013.

Cybersecurity: A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges. GAO-13-462T. Washington, D.C.: March 7, 2013.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO-13-187. Washington, D.C.: February 14, 2013.

Information Security: Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project. Washington, D.C.: GAO-13-155. January 25, 2013.

Information Security: Actions Needed by Census Bureau to Address Weaknesses. GAO-13-63. Washington, D.C.: January 22, 2013.

Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. GAO-12-757. Washington, D.C.: September 18, 2012.

Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy. GAO-12-903. Washington, D.C.: September 11, 2012.

Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices. GAO-12-816. Washington, D.C.: August 31, 2012.

Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape. GAO-12-961T. Washington, D.C.: July 31, 2012.

Information Security: Environmental Protection Agency Needs to Resolve Weaknesses. GAO-12-696. Washington, D.C.: July 19, 2012.

Cybersecurity: Challenges in Securing the Electricity Grid. GAO-12-926T. Washington, D.C.: July 17, 2012.

Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight. GAO-12-479. Washington, D.C.: July 9, 2012.

Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage. GAO-12-876T. Washington, D.C.: June 28, 2012.

Prescription Drug Data: HHS Has Issued Health Privacy and Security Regulations but Needs to Improve Guidance and Oversight. GAO-12-605. Washington, D.C.: June 22, 2012.

Cybersecurity: Threats Impacting the Nation. GAO-12-666T. Washington, D.C.: April 24, 2012.

Management Report: Improvements Needed in SEC's Internal Control and Accounting Procedure. GAO-12-424R. Washington, D.C.: April 13, 2012.

IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. GAO-12-361. Washington, D.C.: March 23, 2012.

Information Security: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data. GAO-12-393. Washington, D.C.: March 16, 2012.

Cybersecurity: Challenges in Securing the Modernized Electricity Grid. GAO-12-507T. Washington, D.C.: February 28, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use. GAO-12-92. Washington, D.C.: December 9, 2011.

Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination. GAO-12-8. Washington, D.C.: November 29, 2011.

Information Security: Additional Guidance Needed to Address Cloud Computing Concerns. GAO-12-130T. Washington, D.C.: October 6, 2011.

Chairman CHAFFETZ. Thank you.

Ms. Tighe, you are now recognized for 5 minutes.

STATEMENT OF KATHLEEN S. TIGHE

Ms. TIGHE. Good morning. Thank you, everyone, for inviting me here today to discuss the work of the U.S. Department of Education Office of Inspector General involving information security and technology security.

The explosion of IT has revolutionized the way the world does business, and the Department is no exception. Virtually every department program relies heavily on information systems. Evaluating whether those information systems are secure is a top priority for my office.

As noted, the Department reports 184 information systems in its inventory, more than 120 of which are operated by contractors or subcontractors, some of which contain sensitive financial information and PII pertaining to millions of students, their parents, and others. These systems are accessed by thousands of authorized individuals, including department employees, contractor employees, and other third parties such as college financial aid administrators.

Protecting its complex IT infrastructure from constantly changing cyber threats is an enormous responsibility and challenge for the Department and its Office of Federal Student Aid. We examine the Department and FSA's information security controls every year through our FISMA audit and in the annual audits of the Department and FSA's financial statements. We also have conducted other IT security-related work.

As detailed in our written testimony, our work has identified deficiencies that impact the security of information within the Department and contractor systems. For example, since 2009, including this year, audits of the Department and FSA's financial statements found persistent IT control deficiencies in key financial systems, including personnel security, access controls, and others.

Since 2011, our FISMA audits have identified weaknesses in security control areas, including a number of repeat findings.

Although our 2015 FISMA audit found that the Department has made progress and has taken steps to address repeat findings, our work determined that more is needed.

This year's FISMA audit had two new features. First, the OIGs were required to evaluate the effectiveness of their agency's security program in the 10 designated FISMA areas for the first time, effectiveness meaning the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome.

Second, the Council of the Inspectors General on Integrity and Efficiency in coordination with OMB and others rolled out the first phase of its new FISMA evaluation metrics called the maturity model, which summarizes the status of information security programs and their maturity on a five-level scale with five being the best. The first phase encompasses the FISMA security area of continuous monitoring management.

Our 2015 FISMA audit found the Department was at level 1 for continuous monitoring management and was not generally effective

in three additional areas: configuration management, incident response and reporting, and remote access management.

Notably, our penetration testing this year revealed a key weakness regarding the Department's ability to detect unauthorized activity inside its computer networks. We determined that three areas were in fact generally effective—risk management, security training, and contingency planning—although some improvements were needed.

Finally, we found that two areas—plans of actions and milestones and identity access management—would be effective if implemented properly, although controls over access to FSA's mainframe environment need improvement.

Although we did not make a separate conclusion on the effectiveness of the Department's program to oversee contractor systems, our review found an issue involving an FSA subcontractor who restricted OIG access to information, which left my office unable to complete a comprehensive vulnerability assessment to determine whether the subcontractor's other customers improperly accessed department data. This is particularly problematic because, based on the information the subcontractor did provide to us, we found accounts with excessive permissions and unauthorized access.

The results of our FISMA and other work show that the Department and FSA must work harder to address existing weaknesses so they can be in a better position to identify and stop increasingly sophisticated attacks on critical IT infrastructures. My office is committed to helping them do so.

Thank you very much. I'm happy to answer questions.

[Prepared statement of Ms. Tighe follows:]

Statement of Inspector General Kathleen S. Tighe
U.S. Department of Education
Before the Committee on Oversight and Government Reform and the
United States House of Representatives
November 17, 2015

Chairman Chaffetz, Ranking Member Cummings, and the members of the Committee on Oversight and Government Reform:

Thank you for inviting me here today to discuss the work of the U.S. Department of Education (Department) Office of Inspector General (OIG) involving information technology security at the Department. The explosion of information technology (IT) has revolutionized the way the world does business—and the Department is no exception. Virtually every Department program relies heavily on information systems. Evaluating whether those information systems are secure and operating effectively is a top priority for the OIG.

The Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA), requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the data and data systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. It also requires inspectors general to annually evaluate agency information security programs and practices. I will focus my testimony on the results of our fiscal year (FY) 2015 FISMA audit, as well as other recent work that my office has conducted related to information security.

Background on the Department's IT Systems and System Security Responsibilities

The Department reports184 information systems in its inventory, more than 120 of which are operated by contractors or subcontractors, some of which contain sensitive financial information and personally identifiable information (PII) pertaining to millions of student aid applicants and recipients, grantees, and others. The following are the key areas and systems that we focused our work on this year:

- The Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) contract established a contractor-owned, contractor operated service model for the Department. Under this contract, Dell Services Federal Government (Dell) provides the network infrastructure and an enterprise-wide IT environment, which includes services such as email, network servers, desktop support, security, and printers.

- The Department's office of Federal Student Aid (FSA) also has a large Virtual Data Center (VDC), currently run by Dell, which serves as the hosting environment for FSA business systems such as 1) the National Student Loan Data System (NSLDS), the central database for Federal student aid, which stores information about loans, grants, borrowers, lenders, schools, services, and guaranty agencies (GAs), and 2) the Central Processing System (CPS), which processes all applications for Federal student aid, calculates financial aid eligibility, and notifies students and educational institutions of the results of the eligibility calculation. Both NSLDS and CPS contain sensitive financial information and PII.

- FSA also relies on the Common Origination Disbursement (COD) system, through which funds to eligible students and schools for the Federal student aid programs are delivered and tracked. COD resides in two data centers: one in Plano, Texas, currently managed by Dell at the VDC, and the second in Columbus, Georgia, managed by Total Systems Services, Inc. (TSYS), under the Department's prime contract with Accenture. Like NSLDS and CPS, the COD system also contains sensitive financial information and PII.

In recent years, the Department has experienced sophisticated attacks on its IT systems, including from hostile websites accessed by employees and phishing campaigns resulting in malware infections, as well credentials stolen from employees or external business partners through keystroke loggers.

Results of Recent OIG Reviews and Investigations

The Department's and FSA's information security controls are examined every year through the OIG's FISMA audit and in the annual financial statement audits of the Department's and FSA's financial statements. We also have conducted other IT-related work outside of our FISMA and financial statement work. All of our work has identified oversight and system deficiencies that impact the security and jeopardize the reliability of information within the Department and contractor systems.

In 2013, I testified before this Committee on recommendations made in OIG reports that the Department had not yet implemented. One area I highlighted was our finding the same deficiencies over and over again, known as repeat findings, particularly in our information

security audits. Since my 2013 testimony, repeat findings continue to be an issue in the area of information security. For example:

- In our FY 2014 FISMA audit, we identified findings in 6 of the 11 security control areas reviewed—configuration management, identity and access management, incident response and reporting, risk management, remote access management, and contingency planning. In addition, in 5 of these 6 areas we had repeat findings from reports issued during the prior 3 years. We also found, in some instances, that although the Department said it had completed its actions to address a recommendation, we continued to find that corrective actions were not implemented. Our FY 2015 FISMA audit identified 6 repeat findings in 4 of 10 areas. I will discuss the results of our FY 2015 FISMA audit in more detail below.

- Likewise, since 2009, including this year, audits of the Department's and the FSA's financial statements, conducted by an independent auditor that the OIG oversees, have found persistent IT control deficiencies in key financial systems. The independent auditor has found that the Department and FSA need to mitigate persistent control deficiencies in the areas of security management, personnel security, access controls, and configuration management across those systems. Failure to correct the deficiencies can increase the risk of unauthorized access to the Department's systems and could affect the reliability and security of the data and information stored in those systems.

The OIG has issued other reports over the last several years that identified issues with the Department's and FSA's oversight and monitoring of information security controls of program participants. For example:

- Our 2014 review of FSA's oversight and monitoring of private collection agencies' (PCA) and GA's information security documents found that FSA did not adequately process PCA system reauthorizations such that PCA's operated without valid authorizations for an average of 8 months, did not ensure that PCAs timely resolved security control deficiencies, and had inadequate assurance that GA information system security complied with the FISMA requirements. PCAs and GAs process Department student loan account records on their own computer systems and connect with various Department systems containing student loan information. FSA has recently taken some steps toward enhancing the security posture of the GAs.

- Our 2013 examination of FSA's Personal Identification Number (PIN) registration system, which provided students and their parents access to their personal records on FSA Web sites, such as fafsa.ed.gov and pin.ed.gov, identified security vulnerabilities that had allowed unauthorized users to access the PIN system. After our review, FSA replaced the PIN system with the more secure Person Authentication Service (PAS) system in May 2015.

FY 2015 FISMA Results

The FISMA evaluations for the OIGs had two new features this year. First, the FISMA Modernization Act of 2014 requires the OIGs this year for the first time to evaluate the effectiveness of their agency's security program and practices. As set forth in National Institute of Standards and Technology (NIST) guidance, "effectiveness" addresses the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome. Second, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with the Office of Management and Budget (OMB), the U.S. Department of Homeland Security, and others, rolled out the first phase of its new FISMA evaluation metrics—the maturity model. The model has as its foundation the NIST effectiveness standard but uses attributes that provide perspective on the overall status of information security within an agency, as well across agencies. It summarizes the status of information security programs and their maturity on a 5-level scale (with 5 being the best). The first phase encompasses the FISMA security area of continuous monitoring management; CIGIE plans to extend the model to other FISMA security areas in 2016.

Our FY 2015 FISMA audit found that the Department was at level 1 for continuous monitoring management, and was not generally effective in three additional areas—configuration management, incident response and reporting, and remote access management. Specifically we found:

- Continuous Monitoring Management: The Department's overall continuous monitoring program only met attributes for level 1 of the CIGIE maturity model, and thus was not

effective. Level 1 means that its continuous monitoring program is ad-hoc—not formalized and activities are performed in a reactive manner. Although the Department defined how it will implement its continuous monitoring activities, related processes, performance measures, policies, and procedures have not been implemented consistently across the Department. However, under OMB requirements, agencies have until FY 2017 to fully implement continuous monitoring of security controls. The Department has developed a project plan to address the timely implementation of a continuous monitoring program that meets NIST requirements. The goal of continuous monitoring is to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Until continuous monitoring is fully implemented, the Department will continue to rely upon manual processes.

- Configuration Management: The Department's configuration management program was not generally effective because of key weaknesses in application connection protocols; unsupported operating systems in the production environment; interface connections operating on expired certificates; inability to detect unauthorized devices connecting to the network; and weaknesses in identifying and resolving configuration management vulnerabilities in the EDUCATE environment. These weaknesses are concerning because they create vulnerabilities that could potentially allow unauthorized users to gain access to Department systems and resources. We also found that although some of the Department's information security policies for configuration management were outdated, they were consistent with NIST requirements; and that the Department has processes for

maintaining and updating inventories for systems, connections, operating systems, and web certificates.

- Incident Response and Reporting: The Department's overall incident response and reporting program is not generally effective because we identified key weaknesses in its internal intrusion detection and prevention of system penetrations. Specifically, during our testing of the EDUCATE environment, OIG testers were able to gain full access to the Department's network and our access went undetected by Dell and the Department's Office of the Chief Information Officer. However, we found the Department was generally effective at ensuring proper incident response and reporting once incidents are reported because it had policies and procedures consistent with NIST requirements; it had established a real-time security operations center; and it had a process that operated to track, monitor, and resolve security incidents. An organization's incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited to prevent future occurrences, and restoring IT services.

- Remote Access Management: The Department's remote access management program was not generally effective mainly because it did not have a complete remote access inventory and did not use two-factor authentication for two of its external network connections. Further, after we notified the Department of this vulnerability, it took approximately 6 months for them to apply two-factor authentication to these two connections. We found that the severity and impact of not enforcing two-factor

authentication on these particular network connections could result in a potential compromise of Department resources.

We determined that three areas—risk management, security training, and contingency planning—were generally effective, although some improvements were needed. For the Department's plan of action and milestones process, we determined that if the established policies and practices are implemented as intended, it should be effective. We also determined that the Department's identity and access management programs and practices would be generally effective if implemented properly, but that the Department's controls over access to FSA's mainframe environment need improvement.

We did not make a separate conclusion on the effectiveness of the Department's program to oversee the security of contractor systems because, given that the Department relies almost exclusively on contractors to operate its systems, our assessment of information security management included in our FISMA report addressed issues of contractor oversight. However, our review specifically found that FSA did not have reasonable assurance that commercial users of a mainframe environment supporting the COD system operated by the subcontractor TSYS do not have access to Department data. During our FISMA audit, TSYS refused to provide the OIG with documentation reflecting a complete listing of all userids with privileges on the mainframe. After repeated requests, TSYS provided a copy of Education userids with privileges, but redacted all other userids with privileges in the mainframe environment. Without this data, the OIG was unable to complete a comprehensive vulnerability assessment of the environment and determine whether other customers on the mainframe could improperly access Department data.

This is particularly problematic because based on the information TSYS did provide regarding the mainframe users, we found accounts with excessive permissions and unauthorized access.

To address the issues identified in our FISMA audit, we made 26 recommendations—16 new recommendations and 10 repeat recommendations, including that the Department direct Accenture to obtain a complete list of userids from TSYS and produce it to FSA and the OIG; and, in the event of refusal or inability to produce the requested information, take appropriate action under the contract or other authority to ensure that Department data hosted by TSYS on the COD mainframe is adequately safeguarded from unauthorized access.

Closing Statement

In light of recent high-profile data breaches at other Federal agencies, the importance of safeguarding the Department's information and information systems cannot be understated. The Department's systems house millions of sensitive records on students, their parents, and others, and facilitate the processing of billions of dollars in education funding. These systems are primarily operated and maintained by contractors and are accessed by thousands of authorized individuals (including Department employees, contractor employees, and other third parties such as school financial aid administrators). Protecting this complex IT infrastructure from constantly changing cyber-threats is an enormous responsibility and challenge. While the Department and FSA have both made progress and taken steps to address past problems that we have identified, our work this year demonstrates once again that they remain vulnerable to attacks and that there are key areas where immediate action and attention are needed. As noted, our penetration testing this year revealed a key weakness regarding the Department's ability to detect unauthorized

activity inside its computer networks that needs to be addressed promptly. Likewise, our work looking at access to data processed on FSA mainframes raises significant concerns over the Department's and FSA's ability to adequately oversee its contractors and ensure that only individuals with appropriate permissions have access to Department data. Our recently issued report highlights numerous areas that need to be improved in order to develop a better IT security program. My office is committed to helping Department and FSA officials strengthen information security controls and mitigate risks to their systems and the valuable data they hold. The Department and FSA must work harder to address existing weaknesses so they can be in a better position to identify and stop ever-evolving cyber threats and increasingly sophisticated attacks on critical IT infrastructures. That concludes my written statement. I am happy to answer your questions.

Chairman CHAFFETZ. Thank you.

Dr. Harris, you are now recognized for 5 minutes.

STATEMENT OF DANNY A. HARRIS

Mr. HARRIS. Thank you, Mr. Chairman.

Chairman Chaffetz, Representative Connolly, and members of the committee, thank you for the opportunity to appear before you today.

As the chief information officer for the Department of Education, I am committed to ensuring we have an effective cybersecurity program in place that includes strong controls and continuously monitors—we continuously monitor and evaluate our posture for opportunities to minimize risk and exposure as we work to improve our current systems and processes.

While ED has made significant progress over the last several years in strengthening the overall cybersecurity program, we are not satisfied and we have solid plans to continue to increase the security of ED's systems. Before I dive into the specifics of our evolution, I wanted to provide brief organizational context that will assist our discussion today.

ED is organized under one department-level CIO, a role that I have served in since 2008. The department-level CIO manages all core IT functions, including but not limited to IT operations, cybersecurity, enterprise architecture, and IT investment management.

The Federal Student Aid, a performance-based organization, also appoints a separate CIO, which reports to FSA's chief operating officer. While the department-level CIO is ultimately accountable for the IT portfolio, FSA maintains independent operational responsibility for its IT portfolio. The FSA enterprise includes major mission systems that support student facing and public services. A few examples include the commonly known Free Application for Federal Student Aid, or FAFSA, and StudentAid.gov.

During my more than 7 years as the Department's CIO, I've worked closely with leadership in FSA to ensure that IT management integrates with the Department's IT systems. Since fiscal year 2011 when the Department was noncompliant with all 10 areas of FISMA, steady and consistent progress has been made.

For example, the Department established a continuing monitoring program to assess the security state of information systems in the Department's two distinct environments, one called EDUCATE, which handles all of our infrastructure services, and the other, FSA's Virtual Data Center.

OCIO and FSA adopted and implemented automated scanning and detection tools to collect, analyze, and report on security-related risks, issues, and threats to the Department's systems. Other improvements include implementation of a network access control, or NAC, which provides device-level authentication and data loss prevention, or DLP, capabilities. This allows for control of data flowing in and out of our environment.

Additionally, the OCIO moved from managed service provider to an in-house security operations center, or what we call a SOC, which allows for real-time threat detection and tracking. As a result, it has gained better situational awareness of its network environment and is able to respond more rapidly to network events.

In July 2015 a two-factor authentication solution for accessing email remotely from personally owned computers and mobile devices replaced the previous user-name-and-password authentication method. The new method meets strong authentication mandates defined by OMB. We have reduced our FISMA noncompliance from 10 metric areas to 5 and have solid plans of resolving the remaining deficiencies.

Most recently, the Department actively worked to address the focus areas of a cyber sprint by completing the review of identification of our high-value assets, completing the indicators of compromised network scan, mitigating critical vulnerabilities, and reviewing and appropriately restricting privileged user access. OCIO and FSA developed implementation plans to increase the issuance of personal identity verification or PIV cards to meet requirements of strong authentication. The OCIO completed its implementation this September, and FSA's completion is scheduled for this December.

OIG's objective for the 2015 FISMA audit changed from a compliance-based auditing approach to a focus on general effectiveness of the Department's IT security program and practices. OIG found that while the Department has made progress in strengthening its information security program with 5 of the 10 reporting metrics noted as generally effectiveness—effective, weaknesses were still noted in four of the five reporting metrics. Specifically, the IG determined it was not generally effective in the areas of continuous monitoring, configuration management, incident response and reporting, and remote access.

In response, we are actively engaged in implementing solutions to address these areas. For example, to meet the requirements of OMB for implementing continuous monitoring by fiscal year 2007, the Department has developed an information security continuous monitoring implementation plan and is actively engaged with DHS to obtain continuous monitoring solutions as part of the task order 2 of the CDM program.

Configuration management activities for fiscal year 2016 include continuing the implementation of our NAC solution, to restrict access for users and devices, strengthen the Department's patch and vulnerability management program and prioritize and update policies and procedures to meet Federal configuration management requirements. For incident response and reporting, the Department is utilizing additional capabilities to identify and block attacks, for example, adding web application firewalls.

And finally, to address weaknesses noted in remote access, the Department continues to consolidate and standardize the remote access solutions currently in use. This will allow for increased consistency in the implementation of controls across the remaining solutions. FSA continues their implementation of two-factor authentication requirements to include two-factor enablement on their remote connections.

Thank you again for the opportunity to testify today and provide you with specifics of our plans. I will be pleased to answer any questions you may have.

[Prepared statement of Mr. Harris follows:]

Statement of Danny Harris, Ph.D.
Chief Information Officer
U.S. Department of Education

Before the U.S. House Oversight and Government Reform Committee

Hearing on
"Agency Compliance with the Federal Information Security Management Act"
November 17, 2015

Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, thank you for the opportunity to appear before you today. As the Chief Information Officer for the Department of Education (ED), I am committed to ensuring we have an effective cybersecurity system in place that includes strong controls. ED continuously monitors and evaluates its posture for opportunities to minimize risk and exposure as we work to improve our current systems and processes. While ED has made significant progress over the last several years in strengthening the overall cybersecurity program, we are not satisfied and have plans to continue to increase the security of ED's systems. Before I dive into the specifics of our evolution, I wanted to provide brief organizational context that will assist our discussion today.

Background

ED is organized under one Department level CIO, a role that I have been serving in since 2008. The Department level CIO manages all core IT functions including but not limited to IT Operations, Cybersecurity, Enterprise Architecture, and IT Investment Management. The Office of Federal Student Aid (FSA), also appoints a separate CIO. While the Department level CIO is ultimately accountable for the IT Portfolio in totality, FSA maintains independent operational responsibility for its portfolio. I work closely with FSA and consult with them on a regular basis. The FSA enterprise includes major mission systems that support student facing and public services. A few examples include the commonly known Free Application for Federal Student Aid (FAFSA) and StudentAid.gov.

The FSA CIO reports to the FSA Chief Operating Officer (COO) and does not report to the Departmental CIO. During my more than seven years as the Department's CIO, I've worked closely with leadership in FSA to ensure that IT Management integrates with the Department's IT systems. I've performed these functions while honoring ED's implementation of the PBO statute. As it stands, my involvement includes oversight and review of FSA IT management activities and review of FSA's budget requests without interfering with FSA's ability to execute its very important operational mission. As required by the Federal IT Acquisition Reform Act (FITARA), we will work to integrate Departmental CIO approvals of FSA as it continues to focus on its critical operations.

In FY 2012, OCIO and FSA established continuous monitoring programs to assess the security state of information systems in the Department's two distinct environments, the Department's Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) system and FSA's Virtual Data Center (VDC) system. To comply with the Office of Management and Budget (OMB) policy, FISMA requirements and applicable National Institute of Standards and Technology (NIST) standards, OCIO and FSA adopted and implemented automated scanning and detection tools to collect, analyze, and report on security-related risks, issues and threats to the Department's information systems and data. The implementation of these continuous monitoring programs was done prior to the Department's participation in the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. This is significant because the Department was one of the early adopters of CDM capabilities. In FY 2015, the Department implemented the core Continuous Monitoring technologies that enable the DHS CDM Phase 1 capabilities of hardware and software management, asset management, vulnerability management, and configuration management. These capabilities further strengthen our cyber security posture.

The Federal Information Security Management Act (FISMA)

Under FISMA of 2002, and its subsequent update in 2014, each year the Department's Office of Inspector General (OIG) conducts an independent evaluation of the Department's overall information technology security program and practices to determine compliance with FISMA requirements. OIG reviews ten (10) metric areas using questions and reporting metrics that DHS provides for each annual review. Since FY2012, the Department, through the actions of the Office of the Chief Information Officer (OCIO) and FSA, continues to address noted deficiencies through corrective actions, and we are continuously working to improve our performance.

We've continued our progress in upgrading our performance and in the FY 2013 FISMA Audit the Department achieved compliance in four (4) metric areas. OIG acknowledged that OCIO had updated identity and access management policies to (1) identify all devices that attach to the network, (2) distinguish devices from users, and (3) authenticate devices that connect to the network consistent with FISMA and NIST guidance. The Department began the implementation of network access control (NAC), data loss prevention (DLP), and other continuous monitoring and diagnostic tools. Additionally, the OCIO moved from a managed service provider to an in-house security operations center (SOC). The SOC allows real-time threat detection and tracking, comprehensive reporting of security events and incidents, vulnerability identification and trending, and incident and remediation tracking. As a result, ED has gained better situational awareness of the network environment and is able to respond more rapidly to network and host-based events.

In FY 2014, the Department was deemed compliant in four (4) metric areas. Specifically, the Department established compliant programs for enterprise-wide continuous monitoring, security awareness training, tracking and monitoring known information security weaknesses, overseeing systems operated on its behalf by contractors or other entities, and security capital planning and investments. As part of the FY 2014 work, the OIG conducted penetration and vulnerability testing of

a major FSA system and noted that, compared with organizations of similar size, the contractor supporting the system was performing a satisfactory job in ensuring that the patches and security configurations of the servers were met.

The Department initiated and completed several activities to improve information security practices in response to and support of the FY 2014 FISMA Audit findings and recommendations. Beginning in May of this year, we implemented three major initiatives over the course of three months.

In May 2015, FSA implemented a new student identification system as part of FSA's Enterprise Identity Management Program (EIMP). FSA's EIMP centralizes all access and identity management functions for non-privileged users and is focused on more efficient and secure provisioning and access management for FSA systems for both privileged and non-privileged users. The Person Authentication Service (PAS) addresses significant former vulnerabilities in the previous FSA PIN system, specifically no longer allowing users to use their social security numbers.

In June 2015, the Department implemented a new Security Operations management system (SecOps) to provide an integrated system to allow joint management of Incident Response. The system capabilities allow for OCIO to respond more quickly to security incidents.

In July 2015, a two-factor authentication solution for accessing email remotely from personally owned desktop or laptop computers and personal mobile devices replaced the previous username and password authentication method, satisfying IG recommendations to strengthen the integrity of the system. This solution meets strong authentication mandates defined by OMB.

OCIO also provided significant dedicated support to OMB's Cybersecurity Sprint interagency working group, created in response to major security breaches in the Federal government. The Department worked with DHS and OMB to develop the

new Federal Cyber Incident Response best practices. The Department has actively worked to address the focus areas of the Cyber Sprint by completing the review and identification of the Department's high-value assets, completing the indicators of compromise network scan, mitigating critical vulnerabilities identified through the DHS Critical Vulnerability Report, and reviewing and appropriately restricting privileged user access. OCIO and FSA developed implementation plans to increase the issuance of personal identity verification (PIV) cards to meet the requirements of strong authentication, especially for privileged users. The OCIO completed implementation of the OCIO plan this September and FSA completion is scheduled for December.

2015 OIG FISMA Audit

OIG's objective for the FY 2015 FISMA Audit changed from a compliance-based auditing approach to a focus on general effectiveness. Under this objective, OIG was to determine whether the Departments' overall information technology security programs and practices were generally effective as they relate to Federal information security requirements. The effectiveness of the Department's security controls is based on the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

OIG found that the Department has made progress in strengthening its information security program, with five of ten reporting metrics noted as generally effective. No conclusion was provided for one metric, Contractor Systems, as the Department relies almost exclusively on contractors to operate its systems, and all of the FISMA aspects of IT security management included in their report implicitly addressed issues on the Department's contractor oversight.

The OIG determined the Department was not generally effective in four areas:

- Continuous Monitoring

- Configuration Management
- Incident Response and Reporting, and
- Remote Access

In response, we are actively engaged in implementing solutions to address these areas.

Continuous Monitoring

Specifically, to meet the requirements of OMB for implementing continuous monitoring controls by FY 2017, the Department has developed an Information Security Continuous Monitoring (ISCM) implementation plan and is actively engaged with DHS through the CDM program to obtain continuous monitoring solutions to enhance the program as part of Task Order 2. Although we were assessed at level 1 of the Council of Inspectors General on Integrity and Efficiency's ISCM maturity model, OIG acknowledged that some of the level 2 activities were met as well.

Configuration Management

Configuration management activities for FY 2016 include continuing the implementation of the Network Access Control (NAC) solution to restrict access for users and devices, strengthening the Department's patch and vulnerability management program, and prioritizing and updating policies and procedures to meet Federal configuration management requirements. Additionally, participation in enterprise-wide asset management activities through the DHS CDM project will strengthen our configuration management program and allow greater visibility into the assets maintained by the Department.

Incident Response and Reporting

For incident response and reporting, the Department is utilizing additional capabilities to identify and block web attacks. The next phases of the Data Loss Prevention (DLP) project scheduled for early FY 2016 will provide greater ability to detect incidents. The Department will also identify gaps in ensuring that the

security capabilities provide full network coverage and determine methods to close those gaps.

Remote Access

To address weaknesses noted in remote access, the Department continues to consolidate and standardize the remote access solutions currently in use. This will allow for increased consistency in the implementation of controls across the remaining solutions. Lastly, FSA continues the implementation of two-factor authentication requirements to include two-factor enablement on their remote connections.

Participation in Department of Homeland Security programs

Finally, the Department participates in and utilizes many DHS programs and services to enhance our security program. As stated earlier, the Department is actively participating in the DHS continuous diagnostics and monitoring program, obtaining tools and services to support and enhance existing continuous monitoring activities. We rely on US-CERT information sharing services to provide early warning notices of compromise activity that the Department needs to include in intrusion monitoring. The Department utilizes DHS scanning and risk assessment services to measure the overall cyber health and hygiene of our cyber environment. Department employees utilize DHS training and education programs, to include general user security awareness training and security role-based courses, to support their cybersecurity roles and meet Federal training requirements. Continuing to utilize these and other services that DHS has to offer – including the EINSTEIN program - is important to the Department as we continue to improve the security of our networks and systems, and provide security guidance and training to our employees.

Conclusion

Thank you again for the opportunity to testify today and provide you with specifics on the work of the Department and our plans to continue to improve the security of our systems, processes and procedures. I would be pleased to answer any questions.

Chairman CHAFFETZ. Thank you. I appreciate that.

I will now recognize the gentleman from Michigan, Mr. Walberg, for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman. Thanks to the panel for being here.

Mr. Harris, I appreciate your testimony and the information you have given. As has been mentioned, DMCS supports back-end loan collection work for borrowers. As CIO rated DMCS as higher risk on the Federal IT Dashboard since at least September 12, 2013, due to contracting problems so severe, a cure notice was even issued. What do you consider when rating the risk of investments on the dashboard? Review that for us.

Mr. HARRIS. Thank you for the question. Thank you for the question.

There are a number of factors that I specifically look at as the CIO to rate an investment. A lot of it has to do with the project management of that investment. In other words, are you meeting deadlines on deliverables? A lot of it has to do simply with the size of the investment. More times than not, an investment can be managed properly, but given the size of it, we still consider it high-risk. In a lot of instances we look at the kinds of data that that system actually maintains. And so not in all instances will you see an investment that is doing well that still won't be perceived as a high risk.

Mr. WALBERG. Based on that, can you then explain why the risk rating went from yellow to dark red in May of 2014, a rating that changed shortly after the House Education and Workforce Committee held a hearing on the problems with DMCS, and why has the rating stayed red through May 2015?

Mr. HARRIS. Representative Walberg, I don't have that information in my head right now, but that's certainly information I'd love to provide you.

Mr. WALBERG. It would be great if you could. Any time frame that you could get that to us?

Mr. HARRIS. Certainly within the week, sir.

Mr. WALBERG. Okay. I appreciate that.

On June 30, 2015, DMCS was re-categorized as low risk. Is your testimony today here under oath that these contracting issues are fully addressed?

Mr. HARRIS. Again, Representative Walberg, I'd have to look at the details of that, and I will get that to you within the week as well.

Mr. WALBERG. Okay. Pretty significant details. We would appreciate that information.

Inspector General Tighe, are you confident that all the problems are fixed and contracting with DMCS is okay based on your work?

Ms. TIGHE. Based on our work, no, I can't say with confidence that everything in DMCS2 is fixed. I mean the contractor Maximus, who is currently operating DMCS2, had a number of problems it needed to fix when it—the contract began a year or so ago. I don't think we can say at this point. We have not audited specifically what Maximus has achieved, but I would find it hard to believe that all the fixes are completed.

Mr. WALBERG. Have you looked at some of the objectives and parameters that they are using, and is there any confidence that flows from that?

Ms. TIGHE. We have not audited the dashboard specifically and what goes into it and whether the analysis related to DMCS2, as put on the dashboard, is correct or not. We've done a number of reports related to DMCS2 dating back a few years. As you probably know, it was a material weakness in the financial statement a few years ago. It's gradually—they've tackled the problems and are able to make DMCS2 functional, at least with workarounds, but I—manual workarounds, but I think the new contractor is supposed to be working on making it fully functional.

Mr. WALBERG. Okay. Thank you. Mr. Chairman, I yield back.

Chairman CHAFFETZ. I thank the gentleman. I now recognize the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. I thank the chair.

Dr. Harris, I have got to say to you it is not confidence-building that you were asked questions by Mr. Walberg involving reports that, you know, going from yellow to red now in a high-risk category, and your answer is I have got to get back to you, seemingly unaware of these reports. Is that your testimony? You were not aware of these reports? This is news to you?

Mr. HARRIS. No, Representative Connolly. It's not news to me. There are—there's a large number of investments that I review. I want to make sure that I provide you accurate information.

Mr. CONNOLLY. Well, it just seems to me if we are going to have a hearing on this subject and you are the CIO, why not be better prepared frankly coming before this committee to be able to answer questions that certainly you could have, should have anticipated.

So in that same pleasant vein, can you address the fact that you got the lowest grade possible in the FITARA scorecard? Understanding it is a work in progress and the intent here is not to put a scarlet letter on one's back, but you really got failing grades in all but one category, and that was a "D". I wouldn't have gotten into graduate school with that kind of scorecard. Please address it.

Mr. HARRIS. Absolutely, sir. I respectfully disagree with the rating. First of all, I am not aware of the source of that information, but what I can tell you, sir, is that we have a solid plan in place, implementation plan in place for FITARA by this December, and, quite frankly, in multiple meetings with OMB they made it very clear to us that our plan was very solid. In fact, many of the requirements of FITARA have already been satisfied by the Department for many, many years. With the exception of FSA, currently all IT operations come through the CIO, specifically spending, for example.

And so I do disagree, respectfully disagree with that report, and I don't know—I haven't found the source of that information yet. But I think we're very solid on FITARA.

Mr. CONNOLLY. Well, I go back to my opening statement. It is not a confidence-building measure to have the CIO saying he disagrees with the findings, and you think you are solid with FITARA when you got an "F". What do you think you should have gotten? The highest grade was a "B" and only two agencies got that.

Mr. HARRIS. I actually think we should have gotten a "C", sir, if I can give you an example of what I mean.

Mr. CONNOLLY. Sure.

Mr. HARRIS. So take the first measure, for example, when you look at data center consolidation. The Department currently, to be real honest with you, we don't own any data centers but our contractors do. But that's beside the point. We still report. We have three data centers, three data centers. And in fact, we will be reducing that to two in fiscal year 2016.

And so it startles me that I see an "F" in data centers when we actually are probably the smallest in the Federal space. And given the amount of data processing we do, I think that's astounding.

Mr. CONNOLLY. I will work with you on that because that happens to be one of my bugaboos. And the Federal Government, as you know, in our last hearing to my surprise we discovered 2,000 more data centers. So the fact that we have a Federal agency testifying they only have three is music to our ears and I will be glad to work with you, Dr. Harris, as I know this committee will, in trying to clarify that ——

Mr. HARRIS. Thank you.

Mr. CONNOLLY.—if that is the case. But let me just say this. I exhort you to do what you can not only in clarifying that grade, but more importantly, the spirit of this is improvement because the object here is to make sure that we don't have the kind of data breach we had at OPM at the Department of Education. And you have a sacred trust in protecting the data of 50 million Americans or more in your care, and, you know, you want to be making the headline that actually your data breach is twice that of, you know, some other agency. And, I mean, that is not your only goal. We want to see you be more efficient. We want you to see IT as a resource and a transformative process.

Why are there, Dr. Harris, repeat recommendations coming out of OIG that haven't been acted on by your office or by the Secretary?

Mr. HARRIS. I concur with the IG, as well as the committee, that repeat findings are always troublesome. There are two reasons why we continue to have some repeat findings.

The first reason is the resolution to some of the findings are quite complex, and they require multiple years to actually resolve. An example, our implementation of our NAC and DLP for the talent that we have, we've spent multiple years implementing NAC and DLP. And in fact, we will finish our implementation this year. But it has taken multiple years to implement those very complex systems. And with the full implementation this fiscal year, we will actually resolve 90 percent of the repeat findings.

Mr. CONNOLLY. And, Ms. Tighe, you would corroborate that?

Ms. TIGHE. We would corroborate that ——

Mr. CONNOLLY. I can't hear you.

Ms. TIGHE. Yes, it has been—we have observed that the NAC solution has taken a long time to fully implement, and it does impact some of our repeat findings.

Mr. CONNOLLY. But you agree with Dr. Harris's statement that by I think you said the end of the year about 90 percent of that will be addressed?

Ms. TIGHE. I don't know if I can agree with that. I mean we haven't audited that conclusion specifically. We'll find out when we go in next year's FISMA audit.

Mr. CONNOLLY. Okay. Thank you. My time is up.

Chairman CHAFFETZ. Will the gentleman yield?

Mr. CONNOLLY. Gladly.

Chairman CHAFFETZ. I want to help clarify this database center issue. You have, best I can tell, 184 information systems, correct?

Mr. HARRIS. That's correct, sir.

Chairman CHAFFETZ. And you have 120 contractors that house that information, correct?

Mr. HARRIS. That is correct, sir.

Chairman CHAFFETZ. So how many data centers do you have?

Mr. HARRIS. We have three data centers that the Department of Education maintains. We have—Federal Student Aid has ——

Chairman CHAFFETZ. How many data centers are there housing this information that you are responsible for?

Mr. HARRIS. I don't know, Mr. Chairman.

Chairman CHAFFETZ. Well, there you go. There is the problem. The answer is not three. You are at least 123, and you don't know? Is a contractor not a database to you?

Mr. HARRIS. I'm sorry. Ask the question again, sir.

Chairman CHAFFETZ. If a contractor is housing the information, is that not a database?

Mr. HARRIS. We do not count that as a data center, sir.

Chairman CHAFFETZ. Why not?

Mr. HARRIS. Based on OMB's guidance on how we count data centers, we don't count that. It—we get that as a service and so we don't count it as a data center.

Chairman CHAFFETZ. So you just contract that out; you leave it alone? The inspector general can't look at it. You don't even consider one of your databases?

Mr. HARRIS. We don't, sir.

Mr. CONNOLLY. So ——

Chairman CHAFFETZ. There is the problem, Mr. Connolly.

Mr. CONNOLLY.—Mr. Chairman, could I just ——

Chairman CHAFFETZ. Sure. Go ahead.

Mr. CONNOLLY. So your philosophy is that a data is compromised through a contractor, that is their problem, not your problem?

Mr. HARRIS. That is not correct.

Mr. CONNOLLY. Well, you can't have it both ways. Either you take responsibility for a data center irrespective of where it is located or you don't. It is under your charge. That is the point I think the chairman is making.

Chairman CHAFFETZ. You are paying for it. We are paying for it. Taxpayers are paying for it.

Mr. CONNOLLY. I mean, fair enough, you don't count it. This isn't a bureaucratic, you know, checklist process. What we are concerned about it efficiency, reliability, and security, and if you have got hundreds or thousands of data centers under the care of contractors, okay, OMB may not count that as technically a Department of Education data center, but it is still in your charge. And our concern here isn't to consolidate for the sake of consolidation so we feel better. It is because we believe it is inefficient to have a multi-

plicity of data centers. In fact, we know it is. And we need cooperation from every agency, irrespective of where they are located.

I yield back, Mr. Chairman.

Chairman CHAFFETZ. And as a concluding point, I hope we could jointly ask that the GAO look at this issue of data centers at the Department of Education.

Mr. WILSHUSEN. I would happy to work with your staff to do that.

Chairman CHAFFETZ. Thank you.

I now recognize the gentleman from North Carolina, Mr. Meadows, for 5 minutes.

Mr. MEADOWS. Thank you, Mr. Chairman. And I thank the ranking member for his insightful questions as it relates to these data centers. I have worked with him in a very close way, in a bipartisan way, and so I find it just very interesting that your testimony here this morning would be that you have three data centers when the GAO would not agree with that. So you are disagreeing with the GAO on their definition, is that correct?

Mr. HARRIS. If GAO is suggesting that we have more—the Department has more than three data centers, yes, sir, I am disagreeing.

Mr. MEADOWS. All right. So here is my concern, Dr. Harris. You know, the headline should read Department of Education Gets an "F". Now, that is not good when we are talking about education, but what is even more troubling is the definition of a data center has been made very clear to me, and I am not a CIO. GAO has been very clear on what they view a data center to be, and under your definition, under your definition, everybody could get rid of every single data center by subcontracting out the service. Do you follow the logic there?

Mr. HARRIS. I do, sir.

Mr. MEADOWS. So are you suggesting that you will go to zero and get an "A" on that dashboard just by subcontracting all your data centers out to someone else?

Mr. HARRIS. No, sir, I do not.

Mr. MEADOWS. Okay. Well, then explain the disconnect to me. Why is your testimony three if indeed you are subcontracting out those services?

Mr. HARRIS. So when OMB does a data call and they give us guidance for how we report ——

Mr. MEADOWS. I am talking about GAO ——

Mr. HARRIS. I'm sorry.

Mr. MEADOWS.—all right, the dashboard. They are going to be the ones that help define this with FITARA and everything else, and we're going to have you back in here on a hearing. So with their definition, how do you think you can consolidate some of those data centers that are subcontracted right now? So do you have 120 subcontracted data centers?

Mr. HARRIS. Sir, the only way to consolidate those is to actually consolidate contracts.

Mr. MEADOWS. Exactly. Thank you, Dr. Harris. And so are you going to consolidate contracts?

Mr. HARRIS. We're certainly willing to take a look at that.

Mr. MEADOWS. Okay. Would I suggest that you do that, because if not, you are going to continue to get an "F" when it comes to data consolidation. The risk is spread across 120 subcontractors. Would you agree with that?

Mr. HARRIS. Yes, sir.

Mr. MEADOWS. Okay. And, Ms. Tighe, were you able to infiltrate their system? I noticed the notes from the fiscal year 2015 indicated that you were able to penetrate the EDUCATE system. Were you able to do that?

Ms. TIGHE. Yes. During our penetration testing for our—the FISMA audit this year, we were able to gain access—full access to the EDUCATE system, which is the general support system that houses a number of the Department's systems, undetected by either the contractor for EDUCATE—Dell—or the CIO's office.

Mr. MEADOWS. So you are saying Dr. Harris didn't know that you were there?

Ms. TIGHE. Correct.

Mr. MEADOWS. So, Dr. Harris, how do you explain—I mean are you willing to stake your reputation and your job on the fact that the system is secure?

Mr. HARRIS. I am today, sir, with full ——

Mr. MEADOWS. So if there is a breach from this point forward, you are willing to resign?

Mr. HARRIS. No, sir, I did not say that.

Mr. MEADOWS. Okay. Well, I said your reputation and your job.

Mr. HARRIS. I certainly will stake my reputation, given where we are today. Our full implementation of NAC and DLP, for example ——

Mr. MEADOWS. So how confident on a scale of 1 to 10 with 10 being the highest are you that we will not have some kind of a breach? Ms. Tighe was able to get in. I have got hackers I could probably hire to get in there today. Wouldn't you agree with that?

Mr. HARRIS. As of today, sir, I would rank it a 7.

Mr. MEADOWS. A 7?

Mr. HARRIS. Yes.

Mr. MEADOWS. So when ——

Mr. HARRIS. We're making great progress but I would rank it a 7.

Mr. MEADOWS. Okay. Now, is this a 7 on the same scale that you just gave yourself a "C" where FITARA gave you—the dashboard gave you an "F"?

Mr. HARRIS. That is correct, sir.

Mr. MEADOWS. All right. So this is the grading according to Dr. Harris?

Mr. HARRIS. I just believe we've made a tremendous amount of progress ——

Mr. MEADOWS. Okay. So what do we tell the 125 million people that have their personal identification numbers potentially at risk when you say that it was a 7, you have staked your reputation on it, and yet we have a breach like we had at OPM? Are you confident that we are not going to have that?

Mr. HARRIS. I have strong confidence, sir, and may I tell you why? Even prior to the cyber sprint where two-factor authentica-

tion required level of assurance 4, long before that, we had two-factor authentication at LOA 3, not as strong as 4 but ——

Mr. MEADOWS. But on two-factor authentication, you went down—it has already been testified you went down. You went the opposite way on our 30-day testing period on, you know, the two-person authentication. So you may have had it but you weren't using it.

Mr. HARRIS. Might I explain?

Mr. MEADOWS. Sure.

Mr. HARRIS. Interestingly enough, two things happened during the cyber sprint. The definition of privileged users changed, and the LOA, the level of assurance, changed. Take a look at the privileged users. The definition went from a technical, hardcore access to technical information to anyone who had access to PII. As a result of that, we voluntarily changed our number to significantly increase the number of privileged users that we were reporting, which dropped our percentage.

Mr. MEADOWS. All right. I appreciate the chair's indulgence. Thank you for your answer. I will yield back.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognize the gentlewoman from New York, Mrs. Maloney, 5 minutes.

Mrs. MALONEY. Mr. Chairman, thank you.

There have been a number of significant data breaches over the past year that have jeopardized the personal and financial information of millions of Americans. Anthem, Premera Blue Cross, the Office of Personnel Management, and most recently, Experian all suffered breaches in which hackers were able to steal the personal information of millions of individuals.

Mr. Harris, we are not here today talking about that kind of massive data breach that has actually happened at the Department of Education, correct?

Mr. HARRIS. That is correct.

Mrs. MALONEY. Okay. The Department of Education systems do contain large volumes of sensitive information, however, including personnel records, financial information on students and borrowers that would be attractive to cyber thieves. Therefore, it is an important part of our oversight to ensure that these systems are adequately protected.

Ms. Tighe, according to the 2015 audit your office issued last Friday, "the Department and FSA made progress in strengthening its information security systems." What are the areas where you have seen the Department make the most progress?

Ms. TIGHE. Some of the areas include—they've done a good job on password controls for system users. They've done a better job—a much better job of—once incidents are found, of reporting them up through US–CERT and addressing those issues. And another area, because we noted in our fiscal year 2014 report, our last year's FISMA report, that there were problems in CIO's office with the fact that they would say they've implemented corrective action, but we would go in the next year and continue to find the same problem even though they said that they did it. They've now implemented a much better process for dealing with corrective action,

and so we've been very pleased to see them actually resolve some issues.

Mrs. MALONEY. Okay. And in your 2015 audit you did identify several weaknesses in the Department's information security system. With respect to those weaknesses, your report states, "we found that the Department was not generally effective in four security areas: continuous monitoring, configuration management, incident response and reporting, and remote access management."

Mr. Harris, as the Department's CIO, do you agree with the IG's assessment that the Department needs improvement in the four security areas I just read?

Mr. HARRIS. Yes, Representative Maloney, I do concur.

Mrs. MALONEY. Okay. Are there any areas in which you disagree with the IG's assessment about the Department's weaknesses in IT security, and if so, what are they?

Mr. HARRIS. No, Representative Maloney, I do not.

Mrs. MALONEY. You do not. Okay. In addition to reporting on weaknesses the IG found in the Department's IT security, the report makes 26 recommendations for improving the effectiveness of the information security programs. Mr. Harris, do you have a timeline for implementing the IG's recommendations?

Mr. HARRIS. Our plan is to resolve all of those recommendations in fiscal year 2016.

Mrs. MALONEY. And when will you have all the recommendations implemented, all of them by the end of 2016?

Mr. HARRIS. That is correct.

Mrs. MALONEY. Okay. Do you have all the tools you need to make the improvements the IG recommended?

Mr. HARRIS. It is a very, very aggressive plan and strategy, but that is surely our intent. If we have to move resources from one place to another, it is certainly our intent to do so.

Mrs. MALONEY. Well, I want to thank you. Given the large amounts of sensitive and confidential information the Department retains, it is imperative that it move as quickly as possible to correct the weaknesses the IG has reported in her report.

Okay. Thank you.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognize the gentleman from North Carolina, Mr. Walker, for 5 minutes.

Mr. WALKER. Thank you, Mr. Chairman.

The inspector general found that the Department's remote access management program was not generally effective because it did not enforce its network timeout requirement or, more significantly, use the two-factor authentication for two of its network connections.

The failure of the Department to enforce the two-factor authentication requirement for remote access users opens it up to the same style of cyber attacks that were used against OPM.

Ms. Tighe, let me start with you if I could please. Can you elaborate on how the Department's failure to enforce timeout requirements in the two-factor process for this remote access opens up the Department of Education to the same attacks potentially that we saw used against the OPM?

Ms. TIGHE. Well, yes. The problem that we identified this year, we had gone out and asked for the inventory—and this was to the

Federal Student Aid organization—what your inventory of remote access devices. They identified four. We did penetration testing, found two more that they didn't even know about, and those two did not have two-factor authentication.

So they have now, we understand—have put two-factor authentication on those two additional remote access points, but we still have, I believe a couple of outstanding recommendations related to remote access. And if you do not have proper controls obviously on remote access, then you do open up the Department to attacks from the outside.

Mr. WALKER. Sure. And I am sure you guys are taking the precaution, you are looking at these two adjustments, modifications, or things that we can include to prevent maybe some more of the cyber attacks. Is that fair to say?

Ms. TIGHE. Yes.

Mr. WALKER. Okay. Dr. Harris, what is the Department of Education—what are your actions and doing to solve this problem? Are you guys doing anything specific to making sure—you know, if I remember correctly, the OPM Director Archuleta ended up having to resign because the breach was so intensive. We don't want the same kind of thing here in the Department of Education. Can you tell me what actions, steps you guys are taking?

Mr. HARRIS. Absolutely, Representative Walker.

So for the two incidents you just mentioned, I concur with the IG. We have since resolved both of those. The incident not passing the buck, I don't have operational responsibility for, but at the end of the day I am accountable and responsible for. And so we have made sure that we continue to harden our two-factor authentication.

And what's really critical is we are looking at least privileged. It's not just a matter of managing your privileged users but making sure they have the minimum privileges that they need. So we're doing both of those.

Mr. WALKER. Would you mind dialing it down just a little bit more specific? When you say you are doing both of those, is there a specific date of implementation? Or how exactly are you doing these things to make sure that it is safer?

Mr. HARRIS. Yes. On the education side we've already completed 100 percent two-factor authentication, LOA 4, the strongest. And on the FSA side of the house, the—their completion date is December of this year.

Mr. WALKER. Okay. Thank you for your answers.

With that, Mr. Chairman, I yield back the balance of my time.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognize the gentleman from Georgia, Mr. Hice, for 5 minutes.

Mr. HICE. Thank you, Mr. Chairman. And thank each of you for being here and testifying.

I would like to begin, Ms. Tighe, with you. According to the 2015 audit, as has already been brought up a couple of times here this morning, there were six repeat findings and 10 repeat recommendations. That, of course, I think, raises a red flag for a lot of people as to why these things are not being addressed. So from your perspective, what is the issue? Is it an inability—are they un-

able to take care of these issues, or is it a matter more of an unwillingness to do so?

Ms. TIGHE. Well, I think there's a lot going on here. There's no one particular reason. I mean some is, as Dr. Harris testified, the fact that sometimes solutions are—can't happen short term. They are sometimes long term. Sometimes we raise issues on particular systems, and they may achieve a solution to that particular problem, but what they don't then do is say, hey, maybe we have the same problem on other systems. So we go back in the next year because we kind of rotate through our work looking at different systems because we can't look at 184 every year, right, so—and sometimes we get to the next year and we see the same problem we identified on this system on another system, which is what, you know, gets frustrating for us.

Mr. HICE. So you would put the blame on this systems rather than ——

Ms. TIGHE. Well ——

Mr. HICE.—an inability or an unwillingness to address the ——

Ms. TIGHE. Well, I think there needs to be a couple of things. I think attention needs to be paid to our recommendations and priority given to them. I think sometimes long-term solutions can seem to happen—be longer than maybe they need to be. And also I think that when we make a recommendation pertaining to one system, it would be good to step back and think—for the Department to step back and think, hey, is this same problem happening on other systems.

Mr. HICE. Okay. Thank you.

Dr. Harris, it appears to me that we're utilizing outdated technology, and I think you have acknowledged that as well. In fact, it appears from what I've read there's 962 operating systems that are no longer supported by vendors. That's inexcusable. The vulnerabilities can't even be spoken of. I mean we can't even fathom the kind of vulnerabilities when you're utilizing technology that's not even supported any longer, and yet you said you feel you'd give yourself a 7 out of 10 that we're currently—how in the world can you give yourself a 7 out of 10 when we're using technology that's not even supported?

Mr. HARRIS. Representative Hice, I would concur with you that it is kind of ridiculous that we're using this old technology. The 7 that I give us is the remediation that we have in place and the tools we have to actually protect those outdated systems while we work hard to catch up. So on the one hand you're absolutely right. There are vulnerabilities on that side, but the remediation is on the side of the tools that we have in place as we modernize.

Mr. HICE. Why is the Department using that old technology?

Mr. HARRIS. A lot of it has ——

Mr. HICE. Why doesn't it catch up with the times?

Mr. HARRIS. Sorry, sir. A lot of it has to do with the system owners and the applications—application owner's ability to keep up with the operating system. In some cases, you have to make a decision do you shut down a mission-critical application that provides services to the public, or do you mitigate the risk? And more times than not we mitigate the risk while we're trying to modernize.

Mr. HICE. All right. So how long is it going to take to modernize?

Mr. HARRIS. I don't have an answer to that, sir, across the entire platform, but I can tell you that we are working hard to do that modernization.

Mr. HICE. All right. So we are going to continue to have vulnerabilities for an indefinite period of time?

Mr. HARRIS. I think we will, sir. And I think what we have to do is work hard to make sure that we have tools in place that mitigates that risk.

Mr. HICE. Okay. "Work hard" sounds fine, Dr. Harris, but what does that mean? When can we expect the system to be secure? We have tens of millions of people whose lives and personal information is at a potential high risk as it relates to vulnerability, and your answer is we are going to work hard. When is the vulnerability going to be removed?

Mr. HARRIS. And, Representative Hice, I would say that we are reasonably secure now. I'm not suggesting that we're not secure, but we do need to strengthen. That's very important. I'm not going to suggest that we don't have a tremendous amount of work to do. But I want—don't want the general public to think that we are not secure.

Mr. HICE. There again, "reasonably" is not a very secure answer. We have got a lot of people whose lives and personal information is potentially hanging in the balance. And this is an issue, Mr. Chairman, that hits every district in this country. And my time is expired but I thank the chairman for this and I yield back.

Chairman CHAFFETZ. I thank the gentleman. I will now recognize the gentlewoman from Illinois, Ms. Kelly, for 5 minutes.

Ms. KELLY. Thank you, Mr. Chairman.

Ms. Tighe, your office identified key weaknesses in the ability of the Department and its contractor Dell to detect and prevent unauthorized access. Can you tell us what your testers were able to do during the vulnerability assessment testing of some of the Department's IT environments?

Ms. TIGHE. Yes. We were able to—during the penetration testing, we were able to gain access—or full access to the complete EDUCATE environment. And EDUCATE, you have to understand, is a—sort of a general support system that houses a number of the Department's systems. So we were able to completely access that and went undetected by either the Department's contractor or the Department.

Ms. KELLY. Thank you. The FISMA audit report explains that the Department's defenses did not detect or terminate the unauthorized access and remained on the network for hours. What kind of risks are the Department's systems exposed to by these weaknesses in detection and prevention of unauthorized access?

Ms. TIGHE. Well, I think the risks would certainly be access to the Department's data. We could have really done anything in there. So the fact that we were able to gain access means that outsiders who have bad intentions are able also to come back through the same way we did and gain access. And that really puts the Department systems and data and employees and everybody who deals with—is involved in our system is at risk.

Ms. KELLY. All right. Mr. Wilshusen, do you know whether this kind of undetected, unauthorized access is characteristic of some of

the major data breaches that have occurred in the public and private sectors?

Mr. WILSHUSEN. Yes, I think it is actually. Indeed, just for example like with the OPM breach, that occurred for a number of months before it was actually detected. And so I think that's often one of the hallmarks of these very successful attacks is that they do go undetected. They exploit known vulnerabilities and systems and then go undetected.

Ms. KELLY. The OIG recommended that the Department ensures its intrusion detection and prevention system and technical security architecture are property configured to restrict and eliminate unauthorized access. Mr. Harris, the Department concurs with this recommendation, correct?

Mr. HARRIS. Yes, we do.

Ms. KELLY. What is the status of the Department's plan, corrective actions, and when do you expect them to be completed?

Mr. HARRIS. So I'm pleased to announce that, with the implementation of our—a NAC system, it allows us to do three things. It allows us to look at all—look and touch all of our assets, it allows us to see the configuration on those assets, and it allows us to manage the vulnerability on those assets. Fiscal year 2016 we plan for a full implementation. It is in place now and we can monitor. The full implementation will allow us to actually block anonymous behavior.

Ms. KELLY. Is this fiscal year 2016 January or March? Around when in fiscal year 2016?

Mr. HARRIS. The third quarter is what we're looking at.

Ms. KELLY. Okay. Thank you. Ms. Tighe, you said in your testimony that the Department was effecting in ensuring proper incident response and reporting once incidents were reported. Can you describe what steps the Department has taken to ensure it effectively responds to incidents?

Ms. TIGHE. Yes, they have—and I would defer to Dr. Harris on this if he has more to add—but I know that they have a SOC, a security operation center, up and running, and that's given them capabilities they never had before in terms of incident reporting and response.

Ms. KELLY. Dr. Harris, did you want to add anything?

Mr. HARRIS. Yes, I would. We have an incident response process that follows both OMB and NIST guidelines, and we also have a very strong and well-documented PIRT process, basically a privacy incidence response team that goes into action when we have breaches.

Ms. KELLY. Okay. And you discussed in your testimony the role of the Department of Homeland Security has in helping the Department identify risks. Can you expand upon that? How do those programs help supplement your efforts?

Mr. HARRIS. Sure. I talk about it in very—I'm very enthusiastic about the progress the Department has made over the last 3 years. A lot of it has to do with the shared services that DHS provides to us, specifically with CDM task order 2 where we will expand our sensors, we will also lower the cost of licensing, and more than anything else, we will have access to dashboards that actually

allow us in real time to look at vulnerabilities. That's what we're missing right now.

Ms. KELLY. Okay. Well, thank you, and I look forward to seeing further progress from all agencies in detecting and responding to incidents. Thank you, and I yield back.

Chairman CHAFFETZ. I thank the gentlewoman.

I will now recognize the chairman of the Subcommittee on IT for our Oversight and Government Reform Committee, the gentleman from Texas, Mr. Hurd.

Mr. HURD. Thank you, Mr. Chairman.

I want to start off with a simple question, and this is to you, Ms. Tighe. When you conduct your penetration testing or technical vulnerability assessment, who decides when that happens? Can the Department come and say, listen, this is a tool we would like to use? Can you do this? Or is this something that you do independently?

Ms. TIGHE. We do it independently.

Mr. HURD. And is that the same across most agencies?

Ms. TIGHE. I think that's the same with most IGs who do penetration testing. I'm not sure everybody does.

Mr. HURD. And how often do you plan on doing penetration testing?

Ms. TIGHE. We do it every year as part of our FISMA audit.

Mr. HURD. Okay. Because that is an industry best practice, and it is a good thing that this is going on. The information you glean is important for Dr. Harris and his team.

Dr. Harris, the remaining of my questions are for you. And I am going to read your statements. And I usually like to dig into the weeds at these hearings, but there is a lot of big-rock strategic issues that have come out here today. In your testimony you say "the department-level CIO"—that is you—"manages all core IT functions, including but not limited to IT operations, cybersecurity, enterprise architecture, and IT investment management." You further add that "the Office of Federal Student Aid (FSA) appoints a separate CIO."

Now, you are saying that you are responsible for all IT department activities but you don't have control over all the activities within the Department of Education. Would that be a true statement?

Mr. HARRIS. That is correct, Representative Hurd.

Mr. HURD. Does that make sense?

Mr. HARRIS. I believe that FITARA will strengthen my ability and authority to actually provide more guidance and oversight, and if you want to use the word control over operations. Right now, that is a challenge.

Mr. HURD. So there are two people missing here today to be frank. Number one is the agency head, right? And I know Arne Duncan has announced his retirement and John King will be taking over as acting duties and I think through the rest of this administration because ultimately, the buck stops there. But we are also missing the CIO of FSA participating in this conversation because it doesn't make any sense.

And we go back to the issue of data centers. Department of Education is ultimately responsible for all the data centers that hold

information for these kids that are applying for Federal aid. So saying that we have three is being disingenuous, right? And my question is, you know, when we have these issues, who is remediating these vulnerabilities, especially when it comes to FSA? Are you responsible for it? Is the CIO of FSA responsible for it? Who is ultimately supposed to be held accountable for these issues?

And you talk about NAC's implementation. Is this going to include all the subcontractors or is this just Department of Education employees that have that on their badge, not necessarily all the subcontractors that work for you?

Mr. HARRIS. Currently, it's just the Department of Education, the latter.

Mr. HURD. Does that make sense?

Mr. HARRIS. No, sir, it does not.

Mr. HURD. So IG reports show that since 2011 there was no mechanism to restrict the use of unauthorized devices on the network. Having the ability to find devices on your network, does it really take 4 years to figure that out?

Mr. HARRIS. With the talent we had, sir, it took us that long ——

Mr. HURD. So you are saying ——

Mr. HARRIS.—and in the last 3 years we've made a tremendous amount of progress.

Mr. HURD. Well, that is not very encouraging. I am hoping we have increased the talent in order to do that because, Ms. Tighe, would you have any opinions on how long it would take to implement one of these systems?

Ms. TIGHE. Well, I would hope it would be done sooner but ——

Mr. HURD. Well, I know ——

Ms. TIGHE.—I—you know, but I would point out that this year's report also highlighted this again as an issue. So to the extent that ——

Mr. HURD. Great. So, Mr. Harris, how many users do you have in the Department of Education?

Mr. HARRIS. Approximately 6,000, sir.

Mr. HURD. Okay. And does that include subcontractors?

Mr. HARRIS. That is correct, sir.

Mr. HURD. So 6,000, just 6,000?

Mr. HARRIS. Yes, sir.

Mr. HURD. Six thousand is not a lot. All right. And I would hope you would share with your CIOs and agency heads—generally, when I ask questions at these hearings, I know the answer because I used to do this for a living, right? And to implement controls on 6,000 users should not take 4 years. I literally thought you were going to say 60,000 or 600,000 users, right? This is completely unacceptable. So who are some of the vendors—so there are 120 contractors? Is that right, Chairman? Or do you know the answer? How many other subcontractors do you have?

Mr. HARRIS. Now, the 6,000 includes just the individuals using the Department's data centers. It does not include the users or the subcontracts outside of the VDC and the ——

Mr. HURD. So why are these subcontractors not under your purview in your responsibility, in your operational control?

Mr. HARRIS. Well, because, for the most part, FSA has contractual arrangements with them. They don't operate their data centers.

Mr. HURD. So why does FSA not—so does Arne Duncan have control over FSA? Does Arne Duncan tell FSA do this and FSA does that?

Mr. HARRIS. I can't answer that, sir. I'd like to get back to you ——

Mr. HURD. So the CIO of FSA, can you tell that person what to do?

Mr. HARRIS. I cannot, sir. That person reports to the COO of FSA. I provide ——

Mr. HURD. And who does ——

Mr. HARRIS.—direction and guidance.

Mr. HURD. And do you know who the COO of FSA reports to?

Mr. HARRIS. Yes, the Secretary.

Mr. HURD. Interesting. I don't even know where to continue. I see my time has expired. But this is the kind of issue that the American people are completely frustrated with. You know, this is not a bureaucratic exercise, as my friend from Virginia pointed out. And saying that Department of Education has a certain level—but you are responsible for all these others, and if you don't have the authority or the power to do that, then you know what, we are here to give you that authority because we want to hold you accountable. But we want to make sure you have all the tools at your disposal to do these things. But it is unacceptable to say 6,000 people. I could probably do that over the weekend. This is completely unacceptable. And I look forward to the hearing tomorrow.

I am sorry, Mr. Chairman, for going over my time. I yield back.

Chairman CHAFFETZ. Thank you. I now recognize myself. To the gentleman from Texas, I would say that I believe we have just in the National Student Loan database 97,000 accounts, 97,000, a little higher than the 6,000. I think you have struck the heart of what is the problem because—one of the problems.

Under the E–Government Act of 2002 and certainly under FITARA, you are supposed to not only have the responsibility but the authority, and I think the gentleman is right. Secretary Duncan needs to answer this.

And my question, how often do you meet with Secretary Duncan?

Mr. HARRIS. On a monthly basis, sir, and ——

Chairman CHAFFETZ. So ——

Mr. HARRIS.—I meet with the deputy secretary weekly.

Chairman CHAFFETZ. So to the gentleman from Texas, I would suggest here they are managing more than $1 trillion in assets, liability for the United States. It is basically the size of Citibank, and the CIO meets with the Secretary maybe 12 times a year, right, once a month?

Mr. HARRIS. That is correct, sir.

Chairman CHAFFETZ. I mean that is absolutely stunning. And looking at the vulnerability of almost half of the population of the United States of America has their personal information sitting in this database, which is not secure by any standard, any scorecard. It is not secure. A trillion dollars, half of all America, and the Sec-

retary of Education, once a month. How long do you meet with him for when you have it? When is the last meeting you had with him?

Mr. HARRIS. About 3 weeks ago, sir.

Chairman CHAFFETZ. How long did you meet with him?

Mr. HARRIS. For an hour-and-a-half.

Chairman CHAFFETZ. Yes. Is it a budget problem? What is your budget? How much money do you have?

Mr. HARRIS. We spend approximately $550 million a year, and about $32 million of that is for IT security.

Chairman CHAFFETZ. How much is for IT security?

Mr. HARRIS. Thirty-two million.

Chairman CHAFFETZ. But ——

Mr. HARRIS. However, there's a large percentage of embedded costs for our contractors that would significantly increase that number ——

Chairman CHAFFETZ. And we will have to work this out with you. My understanding is you spend $683 million on IT at the Department of Education, but do you need more money or do you have enough money?

Mr. HARRIS. Certainly, we could always use more.

Chairman CHAFFETZ. Everybody always says that.

Mr. HARRIS. Sir ——

Chairman CHAFFETZ. Everybody always says that, okay?

Mr. HARRIS. Certainly.

Chairman CHAFFETZ. So ——

Mr. HARRIS. But I would say, sir, that ——

Mr. CONNOLLY. For God's sake ——

Mr. HARRIS.—cybersecurity talent ——

Mr. CONNOLLY.—say yes, Dr. Harris.

Mr. HARRIS. I would say that my biggest challenge is cybersecurity talent even more than money. If you told me to take a choice between the first or the second, I would say you can give me all the money in the world but if the Federal space can't obtain and retain the cyber talent, we are in big trouble.

Chairman CHAFFETZ. No, I absolutely agree with you, and it is something I think this committee needs to look at is the pay authority to perhaps even pay the IT specialists more in such a critical vulnerable situation and the ability in the marketplace to actually attract and retain people. I would agree with you.

Does the Department implement the Department of Homeland Security Continuous Diagnostic and Mitigation system, and do you have the EINSTEIN intrusion detection program thoroughly and completely integrated into all of your IT systems?

Mr. HARRIS. We do, sir. In fact, the Department of Education was one of the first to implement EINSTEIN 1, EINSTEIN 2. We're now working with DHS to implement EINSTEIN 3. And, yes, we do participate in CDM task order 2 specifically.

Chairman CHAFFETZ. Does that include the contractors and subcontractors or ——

Mr. HARRIS. It includes those that run our data center. But it doesn't include some of the partners that FSA has.

Chairman CHAFFETZ. Okay. So who doesn't it include?

Mr. HARRIS. It doesn't include, again, some of the 100 ——

Chairman CHAFFETZ. So if you have 120 contractors ——

Mr. HARRIS. It doesn't include some of them. I would have to get you specific information on, okay, if each one is ——

Chairman CHAFFETZ. If you can follow up with us ——

Mr. HARRIS. Absolutely, sir.

Chairman CHAFFETZ.—and the IG and GAO, that would be great.

Mr. Harris, have you had an intrusion?

Mr. HARRIS. I'm sorry, sir. Say that again.

Chairman CHAFFETZ. Have you had an intrusion? Have you had a data breach?

Mr. HARRIS. We have had both incidents and data breaches. Specifically, in 2015 we had 91 breaches and we had 200—about 250 incidents. We have not in the history of the Department—to my knowledge we have not had a major incident. And so all of them fall into the minor category.

And if I might give you an example of one?

Chairman CHAFFETZ. What was the most significant one?

Mr. HARRIS. I would say, sir, that the most significant one was in 2012 when, in the FAFSA system for a matter of minutes as a result of a—an application glitch, users were able to see other users' PII. And again, it was several minutes, but that's pretty critical.

Chairman CHAFFETZ. Did you report that to the inspector general?

Mr. HARRIS. I'm sure we did, sir.

Chairman CHAFFETZ. In the past year are you aware of any foreign, national, state, or other adversary penetrating the network? Did any of those data breaches and incidents happen in the last year?

Mr. HARRIS. Not in the last year, sir, though we constantly are threatened by them, but no breaches to my knowledge.

Chairman CHAFFETZ. Not in the last year?

Mr. HARRIS. That is correct, sir.

Chairman CHAFFETZ. How many onsite IT security reviews has the Department conducted to date of the contractors that you engage with?

Mr. HARRIS. Our reviews of our contractor are actually constant. We have a security operations center, and we have an IV&V contractor that are working daily to review everything that our contractor is doing.

Chairman CHAFFETZ. Ms. Tighe, what is your view of that?

Ms. TIGHE. I'm aware ——

Chairman CHAFFETZ. Sorry, your microphone.

Ms. TIGHE. I'm aware that the Department is taking those actions. Some parts—I would also point out that some parts of the Department and systems the Department deals with have—and it's external business partners like the Title IV services do get IT general controls reviews every year because they feed into the financial statement audits. So we do have some level of assurance outside of the Department that some—that there is some IT reviews being done of the Department systems.

Chairman CHAFFETZ. All right. Last questions before I recognize Mr. Palmer here, departmental policy requires that all employees and contractors who have access to Privacy Act data have a minimum of a 5c public trust background check, but it is also my un-

derstanding that roughly less than 5,000 of the people who have access have actually had such a background check, which leaves us in the math roughly 85,000 individuals who have had no background check have access to personal information in your databases. Would you disagree with any of those numbers? And what are you doing about it?

Mr. HARRIS. I would not disagree with that information, sir.

Chairman CHAFFETZ. So if it is departmental policy to have background checks for people who have—remember, we are talking about mostly—these are student loans, right? We are talking about students and kids here. So when you are talking about access to private information and it is departmental policy to have a background check, and yet 85,000 of them don't have background check, what are you doing to solve that?

Mr. HARRIS. Sir, I don't believe that includes the individuals who have access to their own information. So the 85,000 you mention aren't system operators who are actually looking at PII. For example, if we have a student looking at their own information, they do not need a 5c clearance.

Chairman CHAFFETZ. Well, no, that number is in the tens of millions of people if not hundreds of millions of people. If they are looking at their own information, I am not counting that. I am talking about people who have access into the system to go look and fish around. And, Ms. Tighe, can you provide more information about that?

Ms. TIGHE. Well, I believe that there are—with access to the National Student Loan database, just taking that database, that there are—our numbers that there are about 97,000 accounts. This is not—these are non-student accounts. Fifty-five thousands of those, we should all realize, are at institutions of higher education because all the financial aid officers in every college and university or other school that receives Title IV funding has to access our databases. And I think that is the biggest area where you're not seeing the background investigations unless that particular college or university requires it themselves. But there are other people who access who have accounts. They're the Title IV servicers, the debt collection entities. There's 22 of those and other assorted people who touch our systems.

Chairman CHAFFETZ. And we know how integrity-failed the debt collection services people are, so, you know, no need for a background check there. That is departmental policy. I need you to get back to us as to what you are doing to rectify that. It is, I think, a huge vulnerability because these are people that are authorized. They have the authentication to get in there, look around, see the personal identifiable information and yet have not had the required background check.

Mr. HARRIS. I will do that, Mr. Chairman.

Chairman CHAFFETZ. Thank you. I have gone well past my time.

I will recognize the gentleman from Alabama, Mr. Palmer, for 5 minutes.

Mr. PALMER. Thank you, Mr. Chairman.

I want to follow up on the question the chairman raised, Dr. Harris, about EINSTEIN. During the IG penetration testing of EDUCATE, why didn't you detect they were on your servers?

Mr. HARRIS. Currently, as I indicated, we have implemented NAC. The full implementation, however, is not complete, and we plan to complete that this fiscal year.

Mr. PALMER. So you are saying ——

Mr. HARRIS. And I do believe we will be able to see that activity then.

Mr. PALMER. Now, I am asking why you didn't detect it when they were on your servers at the time they were doing the penetration testing.

Mr. HARRIS. We didn't have the tools completely configured.

Mr. PALMER. Okay. What tools are you missing?

Mr. HARRIS. We're not missing any. We just don't have them completely configured. For example, NAC has been implemented but there's a lot of configure work—configuration work that needs to be done for full implementation.

Mr. PALMER. So you have the tools but you are not able to apply them?

Mr. HARRIS. We haven't finished the—we haven't completed the configuration of it ——

Mr. PALMER. How ——

Mr. HARRIS.—but we plan to do that this fiscal year.

Mr. PALMER. You should have it done by the end of this fiscal year or the calendar year?

Mr. HARRIS. By the fiscal year, sir.

Mr. PALMER. So they will be complete by September 30 of '16?

Mr. HARRIS. Sir, I'm hoping to complete them by the end of the third quarter, not September 30.

Mr. PALMER. Okay. So that would be ——

Mr. HARRIS. And we're aggressively working to actually do it sooner than that.

Mr. PALMER. All right. They will be finished by the end of June?

Mr. HARRIS. That is correct.

Mr. PALMER. Okay. Thank you. Dr. Harris, according to the Federal IT Dashboard, DOED central processing system carries out data matching with at least five different agencies and interfaces with DOED's Participation Management, Common Origination system, and Virtual Data Center. What is the nature of this understanding between agencies?

Mr. HARRIS. Beyond the sharing of data, that really is the totality of that understanding. We share sensitive data. We share important data with which to do better data processing on both sides.

Mr. PALMER. Well, CPS is not PIV-enabled, and if it were to be breached, an adversary would have access to sensitive personally identifiable information and data that multiple agencies rely on. Can you tell me what security measures are in place to protect the CPS system?

Mr. HARRIS. I apologize, sir. I don't have operational oversight of that system and have limited knowledge, but I can certainly get you more information on that.

Mr. PALMER. Who has that information?

Mr. HARRIS. The Federal Student Aid CIO.

Mr. PALMER. Okay. One last question, do you allow employees to use your server to access their personal email?

Mr. HARRIS. Currently, we do, sir.

Mr. PALMER. Is that not of concern to you on that ——

Mr. HARRIS. It—I'm sorry, sir.

Mr. PALMER. Well, we have had other hearings on this when we were dealing with the breach at OPM, and it turns out that the immigration, ICE, had sent out a memo to their employees that they could no longer use the Federal server because they had multiple breaches, and it turns out that there was a union grievance filed and they weren't able to deny their employees access to their server. And it appears that that is where one of the breaches occurred. I just wonder, as the chairman points out, the enormous number of records that could be accessed, if you are taking any measures to prevent that.

Mr. HARRIS. It's an interesting question, Representative Palmer, and it's one that does concern me. We actually met with OMB and DHS to talk about the risk level of allowing that kind of access. I think the CIO counsel is going to spend more time talking about it, but it is something that concerns me. And you're right, it is a threat factor.

Mr. PALMER. Thank you, Mr. Chairman. I yield the balance of my time.

Chairman CHAFFETZ. I thank the gentleman. I will now recognize Mr. Clay of Missouri for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman.

And, Mr. Wilshusen, the high-risk report GAO released earlier this year noted challenges that both the Federal and private sector face when it comes to securing personally identifiable information. In particular, the 2015 high-risk report pointed to the data breaches at Home Depot and Target as examples of high-profile breaches in the commercial sector. So is it fair to say when it comes to the subject of cybersecurity, GAO has paid attention to what has been occurring in the private sector?

Mr. WILSHUSEN. Yes, it is insofar as these types of incidents occur and demonstrate that it isn't strictly—or cybersecurity and these intrusions is not strictly a government phenomenon.

Mr. CLAY. Now, I understand that when GAO conducted its most recent FISMA report on Federal agencies, it wasn't tasked with evaluating the private sector. I would like to ask you some questions about challenges facing the private sector based on your prior work. Are the weaknesses in cybersecurity you are aware of in the private sector consistent with what GAO found with respect to Federal agencies?

Mr. WILSHUSEN. Our review of information security controls at private sector organizations is somewhat limited primarily to the work that we do in evaluating the security controls of our contractors that support the Federal Government. And what we have found is that those contractors also have security vulnerabilities that are consistent with those that we find on agency-operated systems.

Mr. CLAY. So do you think the Federal Government is ahead of the private sector when it comes to cybersecurity?

Mr. WILSHUSEN. I don't know if I could say that. One thing that I could say is that at least the Federal Government, and particularly in respect to the types of information security policies and guidance that are promulgated by the National Institute of Stand-

ards and Technology is among the best and are sometimes used by private sector organizations.

Mr. CLAY. Okay.

Mr. WILSHUSEN. So we do a pretty good job in identifying policies and procedures. Where we're challenged is implementing them in our information systems controls environments over time throughout the entire enterprise.

Mr. CLAY. Ms. Tighe, would you have anything to add?

Ms. TIGHE. No. I would agree that NIST provides very significant and complete guidelines for IT—in the area of IT security. The challenge is getting them implemented.

Mr. CLAY. Thank you. And, Dr. Harris, anything additional?

Mr. HARRIS. I would absolutely concur. In fact, as we work with some of our private sector partners, we see that they don't use standards as stringent as those that NIST provides.

Mr. CLAY. Thank you all. Thank all of you for your responses. May I yield the balance of my time to the ranking member?

Mr. CONNOLLY. I thank my colleague. By the way, I will throw you a lifeline, Dr. Harris. We have talked a lot of about FSA, but it was Congress acting on the recommendations of a previous administration that actually made FSA a PBO, a performance-based organization, and even referred to it as—FSA is generally siloed from the rest of the Department of Education, although its chief operating officer reports to the Secretary of Education, as Dr. Harris testified.

So it is Congress in legislation that we passed in 1997 on a bipartisan basis, our former colleagues Howard "Buck" McKeon and Dan Kildee who actually authored H.R. 2536 that did that. So we now need, because of the passage of FITARA, frankly to square those two. And I think the current Congress would favor the FITARA approach and maybe look a little askance at siloing anything in light of technology progressing and the threat we are facing.

If the chair would just indulge me one question and then I am done ——

Chairman CHAFFETZ. Sure. Yes.

Mr. CONNOLLY.—if Mr. Mulvaney would—okay. In listening to this hearing, I am not sure we are reassured. We dispute the "F" we get in FITARA. We are not fully aware of these other rankings that move us to high risk or yellow to red. Systems weren't quite in place when the penetration exercise, according to Ms. Tighe, "we could have gone anywhere" in that exercise, very alarming. We only have three data centers but we don't know how many our contractors have and we are not really entirely responsible for that even though they are in possession of data that could be compromised.

Certainly, take the point, Dr. Harris, that we need to bulk up on the talent pool as much as we do resources, but we need both. We need both. There is no question about it.

But at the end of the day, Dr. Harris testified with respect to the question of vulnerability, "we are reasonably secure now. I don't want anyone to think otherwise." I have got to challenge that and I want you, Ms. Tighe, and you, Mr. Wilshusen, to respond to that. My question is should Americans be concerned that the kind of

breach that occurred at OPM frankly could occur with respect to at least 50 million Americans whose data is in the hands of the Department of Education? I am not leaving this hearing feeling that we are reasonably secure now. Professionally, is that your judgment? Do you share Dr. Harris's confidence that we are reasonably secure now?

Ms. TIGHE. I am still concerned about the potential for breaches in the Department. I think that the issues we pointed to in our current FISMA report, particularly under the areas of configuration management and under incident detection are very significant, and they really point to the potential for significant vulnerabilities. There was also the issue on the mainframe in Georgia operated by a subcontractor that we were not even able to properly evaluate. And we found privileged users with permissions not appropriate. That stuff worries me, and I don't feel, you know, as rosy about the picture as Dr. Harris. With all that said, I know the Department is working on these things.

Mr. WILSHUSEN. I would defer to Ms. Tighe in her assessment but also just comment on the types of weaknesses that she and her team identified at Education as being those types of vulnerabilities that can be exploited and can be used to gain access and even, you know, potentially hide an intruder's presence on a network.

Mr. CONNOLLY. I thank the chair and I thank Mr. Mulvaney for his courtesy.

Chairman CHAFFETZ. I will now recognize the gentleman from South Carolina, Mr. Mulvaney.

Mr. MULVANEY. I thank both the gentleman. And I have just got a couple of mopping-up questions here at the end so in no particular order.

Mr. Harris, you mentioned a couple different times talent, which is something we don't hear much in here. Ordinarily, people come in and complain they don't have enough money. I have not heard that one before. Let me ask you this. Do you not have access—my understanding was that in other areas of the Federal Government we have some really, really good people working on IT. Do you not have access to their expertise and their subcontractors and their experiences?

Mr. HARRIS. Thank you so much for the question, Representative Mulvaney.

I'm so glad you raised it because you do have talent across the Federal space, in, fact one of the things I am hoping that this body will help with is actually centralizing some of that talent so a small agency like the Department of Education can get more help. But what the Federal—what the private space is paying we simply can't match that, and in a lot of instances, folks don't see the Department of Education as an exciting cyber space to go to. So we're very challenged when we compete with other Federal agencies, as well as the private space. So we are really hurting from that perspective.

Mr. MULVANEY. And that is sort of what worries me is that because you are not exciting, people actually might be attracted to you in terms of being a target.

Ms. Tighe, I come back to something you said earlier about—and I am going to butcher the numbers—97-odd-thousand users, and

you made an excellent point, which is that there is someone in the registrar's office at G.W. who has access to this system. Let me ask you this. If I am sitting there and I am at G.W. and I am the, you know, little part-time student who comes in to work on the FAFSA stuff, what do I need in order to get Mr. Chaffetz's student loan information?

Ms. TIGHE. Well, you need his—most financial aid administrators—well, you probably need him to either have gone to G.W. University ——

Mr. MULVANEY. Okay.

Ms. TIGHE.—or put that as one of his schools on his application. So ——

Mr. MULVANEY. Okay ——

Ms. TIGHE.—they have a more limited purview than they ——

Mr. MULVANEY. All right. So if I am sitting there ——

Ms. TIGHE.—have access to.

Mr. MULVANEY.—and I am the person at G.W. who is—and I hate to pick on G.W. but I went to Georgetown ——

Ms. TIGHE. Or his Social.

Mr. MULVANEY. Yes. I went to Georgetown so I love to pick on G.W.

Ms. TIGHE. Yes.

Mr. MULVANEY. You are telling me I can only gain access to people who have actually either gone to G.W. or checked that on one of their FAFSA forms?

Ms. TIGHE. Yes, unless they, for whatever reason, would have their Social Security number.

Mr. MULVANEY. And that was my next question ——

Ms. TIGHE. Yes.

Mr. MULVANEY.—which is if I have Mr. Chaffetz's Social Security number and he is in the system, I can get him, can't I?

Ms. TIGHE. That's my understanding.

Mr. MULVANEY. So that means that if I am able to acquire that Social Security number from any other source and I have access to your system at tens of thousands of terminals, I can get just about anything?

Ms. TIGHE. That's correct.

Mr. MULVANEY. Now, let me drill down on that a little bit. What is "just about anything" because when I—I got a little notice from I think it was Target—my wife did—saying that they had been hacked. I get all that. That is right. That doesn't bother me too much. I think we use the same credit card there and I don't use anything else at Target. If you hack into Mr. Chaffetz's records at the Department of Education, what type of information can you get on him?

Ms. TIGHE. Well, you can—obviously, you can get the financial information reported in the application for Federal Student Aid and ——

Mr. MULVANEY. Does that include his parents' income?

Ms. TIGHE. Yes, it does.

Mr. MULVANEY. Does it include any bank account information? We didn't have these forms when I was in school ——

Ms. TIGHE. Do we—is it ——

Mr. MULVANEY.—so I am not really sure ——

Ms. TIGHE.—bank account information? Yes. I think—believe there is banking information.

Mr. MULVANEY. What about stocks and bond account information?

Ms. TIGHE. I wouldn't think that would be available.

Mr. MULVANEY. Okay. All right. What else can you get just out of curiosity?

Ms. TIGHE. Let me get back to you on a full accounting ——

Mr. MULVANEY. Okay.

Ms. TIGHE.—of what the—is available.

Mr. MULVANEY. And I hope I am making my point, which is that when Target got hacked ——

Ms. TIGHE. Yes.

Mr. MULVANEY.—I didn't lose a lot of concern over it. If someone had my bank account records, that might—including, I guess, account numbers because I guess you all at some point verify that information or can ——

Ms. TIGHE. Well, there is information related to the students'—for disbursements as student aid, you know, moving money into the students' bank accounts.

Mr. MULVANEY. Sure. Okay. And I am sorry; I lost track of where I was going after that. So I would be happy to yield to the chair whatever 40 seconds I have left. But I thank you all for your information and looking forward to going forward.

Chairman CHAFFETZ. If the gentleman will yield, there are lifetime loan limits, right? So talk to the scope of time here that we are talking about.

Ms. TIGHE. My understanding is in the National Student Loan database is that once you get money, your information is kept in there for—like I don't think there's a deadline or cutoff for when that information gets moved because there are statutory limits on the amount of student aid one can take so they have to keep track of it over a lifetime. So they—it's—the information is retained for a very long time.

Chairman CHAFFETZ. And how many people in that database?

Ms. TIGHE. There are, I think, currently about 85—at least somewhere over 75 million student accounts or student account information.

Chairman CHAFFETZ. And in addition to that, there are other individuals, right? So how many individuals are we ultimately talking about?

Ms. TIGHE. Well, Student Loan database—the National Student Loan database will have just students who get financial aid. There are other systems the Department has like the CPS system where you will have the parent information also.

Chairman CHAFFETZ. So how many Americans? What is the grand total of number of Social Security numbers—we had ——

Ms. TIGHE. Well, the 130—we—by our count from the OIG's estimation of looking at the Department's databases we have over 139 million unique Social Security numbers. And that's just in the student loan application and the PIN registry systems.

Chairman CHAFFETZ. Does the gentleman yield back?

Mr. MULVANEY. Yes, sir.

Chairman CHAFFETZ. In wrap-up here, I want to address something just to clarify. You have a responsibility, Ms. Tighe, as the inspector general to be able to go in and look at the contractors and the subcontractors, but you have had difficulty gaining access to some of those systems, specifically the COD or the Common Origination and Disbursement system. Have you been able to look at that system?

Ms. TIGHE. No, we were not able to. We included the mainframes of the Department as part of our testing this year. Two of those mainframes are at the Virtual—the VDC, the Virtual Data Center. One of them is in Columbus, Georgia, and operated by a company called TSYS under a subcontract with the Federal Student Aid organization. We entered into an agreement with them that outlined everything we needed. We gave them a timetable.

They did not by any stretch of the imagination meet that timetable, and in the end, they were not able to provide us very critical information for us to do a full vulnerability testing. They limited our information in the end to the education environment. The problem is that mainframe in Georgia is a shared environment with their private customers.

And I understand their reluctance, but the fact remains is, given the problems we found with what—just what they were able to provide us, seeing privileged users that had excessive permissions and the like, I worry about what other users we were not able to see have access to in our data.

Chairman CHAFFETZ. Well, we want to be supportive of the inspector general community and the good people at TSYS. Is that their name? They are about to get a nasty-gram from the United States Congress, and we will use every power we have to yank them up here and make sure that you get the access to that information so ——

Ms. TIGHE. I appreciate it.

Chairman CHAFFETZ.—the folks down there can look forward to that. We are going to make sure you have the access you need.

Mr. Harris, last bit of questions. Talk to me about how dilapidated, outdated some of the operating systems software that you are having to deal with. Do you use a COBOL, for instance?

Mr. HARRIS. No, sir, we do not use COBOL.

Chairman CHAFFETZ. Do ——

Mr. HARRIS. On the FSA side I'm not sure if they still have any COBOL-based systems, but I can get that information for you.

Chairman CHAFFETZ. But all the other systems, you are not aware of any ——

Mr. HARRIS. Do not use COBOL, sir, no.

Chairman CHAFFETZ. Do you use DOS or what ——

Mr. HARRIS. No, sir. We're primarily a Windows-based. We use a lot of Linux, Unix. However, it's not just the operating system; it's the version.

Chairman CHAFFETZ. Sure.

Mr. HARRIS. When you get past N minus 1 and the vendor is no longer patching it, you have a problem.

Chairman CHAFFETZ. So how old—what Windows operating systems are you using? And it is probably a whole gambit, right?

Mr. HARRIS. It's a gambit.

Chairman CHAFFETZ. How old is the worst? I mean if you were to walk around say, oh, my goodness ——

Mr. HARRIS. It's—probably the worst would probably be five versions old.

Chairman CHAFFETZ. So like what is that, Windows 95, 97?

Mr. HARRIS. Probably 97.

Chairman CHAFFETZ. Ninety-seven still? And they are not even servicing that at Microsoft anymore?

Mr. HARRIS. That is correct. That is correct.

Chairman CHAFFETZ. So there are no security patches being updated? The ——

Mr. HARRIS. Not for those, sir, but to be fair, many of the systems using those operating systems do not have sensitive data. I don't want to suggest that there is student information sitting on systems that use Windows 97 but ——

Chairman CHAFFETZ. Understood, but ——

Mr. HARRIS.—these are OSs.

Chairman CHAFFETZ. But you feel for the employee, who is their good, patriotic, hardworking ——

Mr. HARRIS. Sure.

Chairman CHAFFETZ.—employee who is going into work trying to negotiate a Windows 97 operating system as opposed to something a little bit more up-to-date.

Listen, this has been very productive. I appreciate all the work that not only the three of you individually do but that your organizations do. We have got a lot of good people who try to do the right thing, they work hard, and I want to carry back that, you know, how much we care and appreciate them and what they do from the GAO to the inspector general to the Department of Education.

That is the beauty—and I say this often in this committee. The beauty of the United States of America is that the Congress does ask hard questions. That is what we are supposed to be doing. That is what makes us unique in this country is we hold people accountable, we ask hard questions, and we have the good dialogue back and forth.

So I appreciate the attitude and approach, Mr. Harris, that you have had here, but we do ultimately want to not only be the Oversight Committee but the Government Reform Committee. To the extent we can help you with these issues, we want to do that.

Mr. CONNOLLY. And, Mr. Chairman ——

Chairman CHAFFETZ. Happy to yield.

Mr. CONNOLLY.—we do have—thank you, Mr. Chairman. We do have a legislative item that sooner or later we are going to have to review, and that is this apparent conflict between what FITARA is trying to get at, which is to enhance Dr. Harris's authority and responsibility, and the older legislation from 1997 that may have been appropriate when Windows 97 was still operating, but we also need to upgrade our own legislative mandate because Dr. Harris is handicapped by statute. And we may have to address that ——

Chairman CHAFFETZ. And that is where I think the E–Government Act of 2002 is actually what we should be looking at, but I look forward to working with you because ——

Mr. CONNOLLY. Yes.

Chairman CHAFFETZ.—you should have not only the responsibility but the authority, and there should be no discrepancy there. And we will work with you on that.

Again, appreciate the participation of all the members. The committee stands adjourned.

[Whereupon, at 11:51 a.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

November 17, 2015
10 a.m. – Rayburn 2154
Congressman Gerald E. Connolly (VA-11)

Committee on Oversight and Government Reform:
"U.S. Department of Education: Information Security Review"

Mr. Chairman, I appreciate the opportunity to examine the information technology and security programs and practices within the Department of Education and its Federal Student Aid program. The Department might not seem like an obvious target of cyber-related threats, but it is responsible for managing and securing a student loan portfolio of more than $1 trillion, along with the personal information of more than 50 million students between federal loan borrowers, Pell Grant recipients, and other assistance programs. In the wake of the two massive data breaches disclosed by the Office of Personnel Management earlier this year – which collectively put at risk the personal information of more than 28 million current and former federal employees and their families, including Members of Congress like me – every federal agency ought to be reassessing its own information security protocols and reinforcing their efforts to detect and deter cyberattacks and other threats.

Perhaps this should be the first of a recurring set of hearings to gauge successes and shortfalls across agencies when it comes to protecting the vast amount of sensitive information held by the federal government. I think we would find most agencies in a similar situation to the Department of Education, which has made some progress in fortifying its information security defenses in recent years yet continues to struggle with recurring vulnerabilities. In its latest report on the Department's efforts to implement the Federal Information Security Modernization Act (or FISMA), the Inspector General identified 16 findings with 26 recommendations, one-third of which are repeat recommendations. Last year's audit "found that the Department did not perform adequate remediation of weaknesses identified in previous OIG audit reports." While it appears the Department has beefed up its remediation efforts, there still is much work to be done, and I am confident this is not the only Department with these challenges.

This year's audit flagged weaknesses across four key areas: continuous monitoring, configuration management, incident response and reporting, and remote access management. For example, the IG found user accounts, from inside federal employees and outside federal contractors, with excessive or unnecessary permissions and unauthorized access to data. In fact, one of the Department's IT service contractors could not verify to the IG's satisfaction that its other, non-federal customers did not have unauthorized access to the Department's data through a shared service. Even more troubling, the OIG said it was able to not only gain access to the Department's network through a simulated attack, but also launch other attacks on systems connected to the Department while going completely undetected.

Another critical finding in the IG's report that applies to the Department of Education, as well as all federal agencies, is that existing information security protocols if implemented, and implemented consistently throughout the organization, should be effective. Nowhere is this more important than in

cyber security and privacy training for new employees. To be successful here, we must bring about a wholesale cultural revolution so that federal agencies and the workforce understand the critical importance of cyber safety, including basic elements of what many call "cyber hygiene."

Along those same lines, we must hold agencies accountable for implementation of the bipartisan Federal IT Acquisition Reform Act (or FITARA), on which we recently held a hearing and issued a preliminary scorecard for agency progress. One of the key reforms of that legislation, which I was pleased to co-author with the former chairman of this committee, is enhancing CIO authorities to increase transparency and improve risk management to address these very issues. Unfortunately, the Department of Education received an "F" rating on this preliminary assessment based in large part on its self-reporting of few IT investments delivering functionality and their ability to produce savings. I look forward to hearing from CIO Harris about steps he's taking to address both FISMA and FITARA challenges.

The severity of recent data breaches in both the public and private sectors in recent years underscores the urgency for federal agencies and Congress to get serious about investing in IT solutions that better secure our data and taking actions that will be a deterrent for hackers. This is a challenge that has confounded both Democratic and Republican Administrations. The number of IT security incidents reported by federal agencies increased from 5,503 in 2006 to 67,168 in 2014 -- an increase of 1,121 percent!

Unfortunately, these attacks on our private industries and government simply reflect the new normal of the 21st Century, where nation-states represent advanced and persistent threats against one another, constantly seeking to gain unauthorized access to sensitive and classified information on each other's people, intellectual property, and sensitive security information. The likes of North Korea, China, Russia, and Iran are increasingly testing the waters and becoming emboldened by a lack of reprisal or deterrence.

The House earlier this year did pass two bills on a bipartisan basis to encourage voluntary sharing of information between the public and private sectors, but information sharing alone is not enough. We need to get serious about strengthening our cyber workforce, both within the federal government and among our private sector partners. We also need to devise more effective data breach notification policies. As my colleagues know, it's now been almost four months since the breach on background records was announced and notifications are still being made.

So, Mr. Chairman, I appreciate this opportunity to look at what the Department of Education is doing right, and what it can improve upon, with respect to securing its data, but it cannot be the only one. Successfully detecting, defending, and deterring cyber threats, will take a concerted effort across all agencies and among our private partners.

House Oversight and Government Reform
FITARA Implementation Scorecard

November 2015 Grades:

Agency	Data Center Consolidation	IT Portfolio Review Savings	Incremental Development	Risk Assessment Transparency	Overall Grade
EDU	F	F	F	D	F

FY 2015 Q2 (4/15) vs. Cybersecurity Sprint Results (7/29)

CFO Act Agency*	Identity, Credential, and Access Management (Strong Authentication)								
	All Users			Privileged Users			Unprivileged Users		
	FY 15 Q2 (4/15)	Cyber Sprint Results	Change +/-	FY 15 Q2 (4/15)	Cyber Sprint Results	Change +/-	FY 15 Q2 (4/15)	Cyber Sprint Results	Change +/-
GSA	**94**	**99**	*+5*	0	**96**	*+96*	99	**99**	*0*
OPM	**42**	**97**	*+56*	100	**100**	*0*	41	**97**	*+56*
DOT	**32**	**97**	*+65*	67	**100**	*+33*	32	**97**	*+65*
DHS	**87**	**90**	*+3*	41	**97**	*+56*	88	**90**	*+2*
Interior	**43**	**89**	*+46*	21	**100**	*+79*	45	**88**	*+43*
Commerce	**77**	**88**	*+11*	97	**93**	*-4*	76	**88**	*+12*
Treasury	**63**	**88**	*+24*	3	**99**	*+96*	66	**87**	*+21*
NSF	**59**	**86**	*+26*	51	**99**	*+48*	60	**85**	*+25*
HHS	**76**	**84**	*+8*	43	**96**	*+53*	78	**83**	*+5*
SSA	**83**	**83**	*0*	99	**99**	*0*	82	**82**	*0*
DOD	**87**	**82**	*-5*	38	**58**	*+20*	88	**83**	*-5*
VA	**10**	**81**	*+71*	0	**100**	*+100*	10	**80**	*+70*
EPA	**56**	**80**	*+23*	0	**96**	*+96*	61	**77**	*+16*
NRC	**0**	**78**	*+78*	0	**84**	*+84*	0	**78**	*+78*
NASA	**0**	66	*+66*	0	**55**	*+55*	0	**66**	*+66*
Labor	**0**	65	*+65*	0	**68**	*+68*	0	**65**	*+65*
ED	**71**	57	*-14*	14	**11**	*-3*	76	**77**	*+1*
HUD	**0**	46	*+46*	0	**86**	*+86*	0	**45**	*+45*
SBA	**0**	44	*+44*	0	**63**	*+63*	0	**43**	*+43*
USDA	**15**	35	*+20*	6	**69**	*+63*	15	**33**	*+18*
Justice	**36**	31	*-5*	26	**83**	*+57*	36	**30**	*-6*
State	**3**	28	*+25*	21	**76**	*+55*	2	**26**	*+24*
USAID	**19**	23	*+4*	0	**100**	*+100*	20	**21**	*+1*
Energy	**32**	12	*-20*	8	**13**	*+5*	34	**11**	*-23*

* Agencies are sorted based on Cyber Sprint All User Results

CAP Goal Key
FY 15 Q2 target: "All Users"=75%
Meets or exceeds target
Does not meet target

Source: FISMA Data Agency Level Questions 5.1, 5.2.5, 5.3. & 5.4.5 (FY 14 Q4) and 2.1, 2.1.1, 2.2, 2.2.1 (FY 15 Q1) from CyberScope

Note: All Sprint References are as of 7/29 at 4PM