NIST'S PHYSICAL SECURITY VULNERABILITIES: A GAO UNDERCOVER REVIEW

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT &
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

October 11, 2017

Serial No. 115–31

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
27–178PDF WASHINGTON : 2018

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 SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
DANA ROHRABACHER, California
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
STEPHEN KNIGHT, California
BRIAN BABIN, Texas
BARBARA COMSTOCK, Virginia
GARY PALMER, Alabama
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
DRAIN LAHOOD, Illinois
DANIEL WEBSTER, Florida
JIM BANKS, Indiana
ANDY BIGGS, Arizona
ROGER W. MARSHALL, Kansas
NEAL P. DUNN, Florida
CLAY HIGGINS, Louisiana

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
ALAN GRAYSON, Florida
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
DONALD S. BEYER, JR., Virginia
JACKY ROSEN, Nevada
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
PAUL TONKO, New York
BILL FOSTER, Illinois
MARK TAKANO, California
COLLEEN HANABUSA, Hawaii
CHARLIE CRIST, Florida

SUBCOMMITTEE ON OVERSIGHT

HON. DRAIN LAHOOD, Illinois, *Chair*

BILL POSEY, Florida
THOMAS MASSIE, Kentucky
GARY PALMER, Alabama
ROGER W. MARSHALL, Kansas
CLAY HIGGINS, Louisiana
LAMAR S. SMITH, Texas

DONALD S. BEYER, Jr., Virginia, *Ranking Member*
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. BARBARA COMSTOCK, Virginia, *Chair*

FRANK D. LUCAS, Oklahoma
RANDY HULTGREN, Illinois
STEPHEN KNIGHT, California
DARIN LAHOOD, Illinois
RALPH LEE ABRAHAM, Louisiana
DANIEL WEBSTER, Florida
JIM BANKS, Indiana
ROGER W. MARSHALL, Kansas
LAMAR S. SMITH, Texas

DANIEL LIPINSKI, Illinois
ELIZABETH H. ESTY, Connecticut
JACKY ROSEN, Nevada
SUZANNE BONAMICI, Oregon
AMI BERA, California
DONALD S. BEYER, JR., Virginia
EDDIE BERNICE JOHNSON, Texas

CONTENTS

October 11, 2017

Page

Appendix I: Answers to Post-Hearing Questions

NIST'S PHYSICAL SECURITY VULNERABILITIES: A GAO UNDERCOVER REVIEW

Wednesday, October 11, 2017

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:14 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Darin LaHood [Chairman of the Subcommittee on Oversight] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

NIST's Physical Security Vulnerabilities: A GAO Undercover Review

Wednesday, October 11, 2017
10:00 a.m.
2318 Rayburn House Office Building

Witnesses

Ms. Lisa Casias, Deputy Assistant Secretary for Administration, U.S. Department of Commerce

Dr. Kent Rochford, Acting Director, National Institute of Standards and Technology

Mr. Seto Bagdoyan, Director, Audit Services, Forensic Audits & Investigative Service, U.S. Government Accountability Office

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HEARING CHARTER

October 6, 2017

TO: Members, Subcommittee on Oversight and Subcommittee on Research and Technology

FROM: Majority Staff, Committee on Science, Space, and Technology

SUBJECT: Joint Subcommittee Hearing: "NIST's Physical Security Vulnerabilities: A GAO Undercover Review"

The Subcommittee on Oversight and the Subcommittee on Research and Technology of the Committee on Science, Space, and Technology will hold a joint hearing titled *NIST's Physical Security Vulnerabilities: A GAO Undercover Review* on Wednesday, October 11, 2017, at 10:00 a.m. in Room 2318 of the Rayburn House Office Building.

Hearing Purpose:

The purpose of this hearing is to examine the Government Accountability Office's (GAO) report on physical security concerns at the National Institute of Standards and Technology (NIST), conducted at the request of Chairman Smith and Chairman Thune of the Senate Committee on Commerce, Science, and Transportation. This hearing will focus on the prior NIST campus security breaches and vulnerabilities as they relate to the structure and organization of the physical security program at NIST.

Witness List

- **Ms. Lisa Casias**, Deputy Assistant Secretary for Administration at U.S. Department of Commerce
- **Dr. Kent Rochford**, Acting Under Secretary of Commerce for Standards and Technology and Acting Director at National Institute of Standards and Technology
- **Mr. Seto Bagdoyan**, Director, Audit Services, Forensic Audits & Investigative Service at U.S. Government Accountability Office

Staff Contact

For questions related to the hearing, please contact Drew Colliatie or Tom Connally of the Majority Staff at 202-225-6371.

Chairman LAHOOD. The Subcommittee on Oversight and the Subcommittee on Research and Technology will come to order.

Without objection, the Chair is authorized to declare recesses of the Subcommittee at any time.

I want to welcome everyone to today's hearing titled "NIST, the National Institute of Standards and Technology, Physical Security Vulnerabilities: a GAO Undercover Review." I have a few brief remarks before we move into opening statements.

Committee Members and staff just viewed three short videos produced by GAO. At the request of the Department of Commerce, these videos have been labeled law enforcement sensitive, which means the agency has determined that they contain sensitive but not classified information. I remind Members that while they may ask questions today concerning GAO's investigation, witnesses may respond but there are answers that can only be addressed in a closed, non-public setting. Please be mindful of this fact here today.

I would like to instruct the witnesses to answer to the best of their ability, but should an answer call for sensitive information, it may be addressed when we move into executive session at the end of the hearing.

We will now vote to authorize the Subcommittees to enter into executive session at the end of the hearing.

The CLERK. Mr. LaHood.

Chairman LAHOOD. Pursuant to House Rule 11(g)(2), I move that upon completion of all present members' questions under the five minute rule, the remainder of the hearing be closed to the public because the disclosure of the testimony to be heard may compromise sensitive law enforcement information. The clerk will call the roll.

The CLERK. Mr. LaHood?

Chairman LAHOOD. Yes.

The CLERK. Mr. LaHood votes aye.

Mrs. Comstock?

Mrs. COMSTOCK. Aye.

The CLERK. Mrs. Comstock votes aye.

Mr. Lucas?

[No response.]

The CLERK. Mr. Hultgren?

[No response.]

The CLERK. Mr. Posey?

[No response.]

The CLERK. Mr. Massie?

[No response.]

The CLERK. Mr. Knight?

[No response.]

The CLERK. Mr. Loudermilk?

Mr. LOUDERMILK. Aye.

The CLERK. Mr. Loudermilk votes aye.

Mr. Abraham?

[No response.]

The CLERK. Mr. Webster?

[No response.]

The CLERK. Mr. Banks?

Mr. BANKS. Aye.

The CLERK. Mr. Banks votes aye.
Mr. Marshall?
Mr. MARSHALL. Aye.
The CLERK. Mr. Marshall votes aye.
Mr. Higgins?
Mr. HIGGINS. Aye.
The CLERK. Mr. Higgins votes aye.
Mr. Norman?
Mr. NORMAN. Aye.
The CLERK. Mr. Norman votes aye.
Mr. Beyer?
Mr. BEYER. Aye.
The CLERK. Mr. Beyer votes aye.
Mr. Lipinski?
Mr. LIPINSKI. Aye.
Mr. Lipinski votes aye.
Ms. Bonamici?
Ms. BONAMICI. Aye.
Ms. Bonamici votes aye.
Mr. Bera?
[No response.]
The CLERK. Ms. Esty?
Ms. ESTY. Aye.
The CLERK. Ms. Esty votes aye.
Ms. Rosen?
[No response.]
The CLERK. Mr. McNerney?
Mr. MCNERNEY. Aye.
The CLERK. Mr. McNerney votes aye.
Mr. Perlmutter?
[No response.]
The CLERK. Mr. Chairman, 12 Members voted aye. No Members voted nay.
Mr. PERLMUTTER. Aye.
The CLERK. Mr. Perlmutter votes aye. Thirteen Members voted aye. No Members voted nay.
Chairman LAHOOD. There being 13 ayes and zero nos, the motion is agreed to.
Once Members have finished their questioning under the five minute rule, the clerk will clear the room. Only Members of Congress, their staff, and the witnesses may remain in the hearing room.
At this time I recognize myself for five minutes for an opening statement.
Again, good morning and welcome everyone to today's joint subcommittee hearing titled "NIST's Physical Security Vulnerabilities: A GAO Undercover Review."
Today we intend to discuss and evaluate GAO's report on its assessment of the physical security program at NIST, the public version of which is being released in conjunction with this hearing. We will hear from GAO about the questions it sought to answer in undertaking its assessment, as well as the methods it used to assess the current physical security program at NIST. We will also look at GAO's findings and the recommendations it has made with

respect to the physical security program, and the steps NIST management must take to satisfy these recommendations and fortify its physical security.

Finally, as part of today's hearing, we will examine specific instances where physical security at NIST has failed, specifically, an explosion that occurred in July 2015 at the NIST campus in Gaithersburg, Maryland, which was caused by a security officer's attempt to illegally manufacture methamphetamine inside a NIST laboratory, and served as the catalyst for the Committee's investigation of physical security at NIST.

However, before we get to that discussion, in light of transparency, I would like to describe briefly for the public what occurred during the closed portion of today's hearing.

Prior to gaveling into this open session, Members of the Committee examined video evidence of recent physical security breaches at NIST campuses. These videos, captured as part of GAO's covert vulnerability testing, reveal NIST employees failing to adhere to established physical security policies. One video in particular shows an undercover GAO agent subverting detection by security personnel by employing very basic espionage techniques. The evidence produced in these videos shines a light on the porous nature of NIST's physical security, and are particularly concerning to the Committee, especially in light of the fact that the July 2015 meth lab explosion served to put NIST on notice that its physical security program was flawed.

While all of this is discussed in the sensitive version of GAO's report, it is discussed only briefly in the public version being released today, and while certain information is undoubtedly sensitive and must remain concealed from those who would use it for nefarious purposes, nothing I just explained rises to that level. In fact, I believe that this information is vital to ensuring that such breaches are prevented in the future at NIST and other federal agencies.

Before concluding, I would like to focus briefly on some positive aspects of GAO's report. Specifically, the report indicates that the Commerce Department agreed with all of GAO's recommendations, which is the first step toward implementation. Additionally, the report emphasized that NIST has taken some steps to further notify and improve its physical security program. Specifically, GAO found that NIST management had three independent assessments of its physical security program conducted following the July 2015 incident, and that NIST has current plans to implement new physical security policies and procedures as the result of those assessments.

The work that NIST performs is extremely valuable to our Nation. From development of the Cyber Framework to standards used throughout industry and academia alike, NIST's work must continue to thrive. In doing so, however, we must ensure the safety and security of those endeavoring to carry out the NIST mission, just as we must ensure the protection of physical and intellectual assets entrusted to NIST's care.

I look forward to hearing from our witnesses about the status of these new policies and procedures, steps taken toward their implementation, and what NIST and the Department of Commerce intend to do in order to carry out GAO's recommendations.

[The prepared statement of Chairman LaHood follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
October 11, 2017

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement from Chairman Darin LaHood (R-Ill.)

NIST's Physical Security Vulnerabilities: A GAO Undercover Review

Chairman LaHood: Good morning and welcome to today's joint subcommittee hearing: "NIST's Physical Security Vulnerabilities: A GAO Undercover Review."

Today we intend to discuss and evaluate GAO's report on its assessment of the physical security program at NIST—the public version of which is being released in conjunction with this hearing.

We will hear from GAO about the questions it sought to answer in undertaking its assessment, as well as the methods it used to assess the current physical security program at NIST.

We will also look at GAO's findings and the recommendations it has made with respect to the physical security program, and the steps NIST management must take to satisfy these recommendations and fortify its physical security.

Finally, as part of today's hearing, we will examine specific instances where physical security at NIST has failed. Specifically, an explosion that occurred in July 2015 at the NIST campus in Gaithersburg, which was caused by a security officer's attempt to illegally manufacture methamphetamine inside a NIST laboratory, and served as the catalyst for the Committee's investigation of physical security at NIST.

However, before we get to that discussion—in light of transparency—I would like to describe briefly for the public what occurred during the closed-portion of today's hearing.

Prior to gaveling into this open-session, Members of the Committee examined video evidence of recent physical security breaches at NIST campuses. These videos, captured as part of GAO's covert vulnerability testing, reveal NIST employees failing to adhere to established physical security policies. One video in particular shows an undercover GAO agent subverting detection by security personnel by employing very basic espionage techniques.

The evidence produced in these videos shines a light on the porous nature of NIST's physical security, and are particularly concerning to the Committee, especially in light

of the fact that the July 2015 meth lab explosion served to put NIST on notice that its physical security program was flawed.

While all of this is discussed in the sensitive version of GAO's report, it is discussed only briefly in the public version being released today. And while certain information is undoubtedly sensitive and must remain concealed from those who would use it for nefarious purposes, nothing I just explained rises to that level. In fact, I believe that this information is vital to ensuring that such breaches are prevented in the future at NIST and other federal agencies.

Before concluding, I would like to focus briefly on some positive aspects of GAO's report. Specifically, the report indicates that Commerce agreed with all of GAO's recommendations, which is the first step toward implementation.

Additionally, the report emphasized that NIST has taken some steps to further fortify and improve its physical security program. Specifically, GAO found that NIST management had three independent assessments of its physical security program conducted following the July 2015 incident, and that NIST has current plans to implement new physical security policies and procedures as the result of those assessments.

The work that NIST performs is extremely valuable to our nation. From development of the Cyber Framework to standards used throughout industry and academia alike, NIST's work must continue to thrive. In doing so, however, we must ensure the safety and security of those endeavoring to carry out the NIST mission, just as we must ensure the protection of physical and intellectual assets entrusted to NIST's care.

I look forward to hearing from our witnesses about the status of these new policies and procedures, steps taken toward their implementation, and what NIST and Commerce intend to do in order to carry out GAO's recommendations.

###

Chairman LAHOOD. I now recognize the Ranking Member, the gentleman from Virginia, for his opening statement.

Mr. BEYER. Thank you very much, and thank you, Chairman LaHood and Chairwoman Comstock for calling this meeting. Thanks to all of you for being here.

The National Institute of Science and Standards and Technology is a vital federal science agency that for more than a hundred years has helped push American innovation in areas as diverse as computer chips, nanoscale devices, the smart electric power grid, and earthquake-resistant skyscrapers. The advanced technologies being developed and pioneering research being conducted at NIST makes security of its facilities and technologies critically important.

Unfortunately, security at NIST at both the Gaithersburg, Maryland, and Boulder, Colorado, campuses has been a struggle. As Chairman LaHood pointed out, in July 2015, a NIST police officer attempting to brew methamphetamine in a little-used laboratory on the Gaithersburg campus was injured in an explosion. He was subsequently arrested, fired, and is currently serving a 41-month prison sentence. In April 2016, a non-NIST employee gained access to a secure lab on NIST's Boulder, Colorado, campus. In May 2017, a paraglider landed on the grounds of the Colorado campus, and in June 2017 a member of NIST's police force was arrested and charged with first- and second-degree assault by the Frederick County Sheriff's Department in Maryland.

Today, we'll discuss the GAO's recent security review at both campuses, and this showed significant issues with NIST's security structure, operating procedures, and performance. Security awareness training for NIST employees should be increased, and the agency's guard force must improve their attentiveness to potential threats, the effectiveness of NIST's security procedures must be thoroughly assessed, and a comprehensive communication strategy that can help identify and resolve potential security threats should be implemented.

My biggest concern regarding security at NIST is the security structure. It's fragmented, inefficient and in some cases inadequate. The Department of Commerce oversees the security personnel at NIST who implement physical security policies, for example, while NIST manages access control technologies and other physical security countermeasures. This security structure violates best practice for security, which calls for centrally managing physical security assets and operations. Without a cohesive organizational structure, it seems inevitable that gaps in security will continue to emerge, and the management of NIST's security will be inefficient and potentially ineffective.

GAO in its review pointed out further problems with NIST security management that we'll hear about, but it's also worth noting the positive stuff, that NIST has made positive commitment to improving security. Seventy-five percent of NIST staff surveyed by GAO believed that NIST's leadership places a great or very great importance on security issues, and this commitment to security is really encouraging, but I expect the leadership at the Department of Commerce and NIST to work together to fully and quickly address the issues outlined.

You know, the science and technology research and programs carried out at NIST helps U.S. businesses grow, it strengthens the U.S. economy, and expands our scientific and technical knowledge. So we in Congress and the public expect NIST to not only protect their vital resources, and in some cases hazardous materials, from potential threats, but also to protect NIST's employees, visiting scientists and others from physical security risks.

I'd like to point out that the Acting Director, Dr. Kent Rochford, only stepped into this role in January, so thank you for being here today and helping tell us how you plan to address these issues.

And finally, I'd like to note my disappointment, the disappointment of our Minority team with the Department of Commerce and NIST for their late submittal of the testimony less than 24 hours ago, despite a 48-hour deadline. And both Majority and Minority I think were surprised that the joint written testimony came from both Commerce and NIST, and perhaps you can talk about that in your testimony.

So Chairman LaHood, thank you very much for calling this meeting. Thank you to all of our witnesses, and we look forward to a productive meeting.

[The prepared statement of Mr. Beyer follows:]

OPENING STATEMENT
Ranking Member Don Beyer (D-VA)
of the Subcommittee on Oversight

House Committee on Science, Space & Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
"NIST's Physical Security Vulnerabilities: A GAO Undercover Review"
October 11, 2017

Thank you Chairs LaHood and Comstock for holding this hearing today.

The National Institute of Standards and Technology or NIST is a vital federal science agency that, for more than one hundred years, has helped push American innovation in areas as diverse as computer chips, nanoscale devices, the smart electric power grid and earthquake-resistant skyscrapers. The advanced technologies being developed and pioneering research being conducted at NIST makes security of its facilities and technologies critically important.

Unfortunately, security at NIST – on its Gaithersburg, Maryland and Boulder, Colorado campuses – has been a struggle. In July 2015, a NIST police officer attempting to brew methamphetamine in a little used laboratory on the Gaithersburg campus was injured in an explosion. He was subsequently arrested, fired, and is currently serving a 41 month prison sentence. In April 2016, a non-NIST employee gained access to a secure lab on NIST's Boulder, Colorado campus. In May 2017, a paraglider landed on the grounds of the Colorado campus, and in June 2017 a member of NIST's police force was arrested and charged with 1st and 2nd degree assault by the Frederick County Sheriff's Department in Maryland.

Today, we will discuss the Government Accountability Office's (GAO's) recent security review of NIST at both campuses. The review showed significant issues with NIST's security structure, operating procedures, and performance. Security awareness training for NIST employees should be increased, the Agency's guard force must improve their attentiveness to potential threats, the effectiveness of NIST's security procedures must be thoroughly assessed, and a comprehensive communication strategy that can help identify and resolve potential security threats should be implemented.

My biggest concern regarding security at NIST is the Agency's security structure. It is fragmented, inefficient and in some cases inadequate. The Department of Commerce oversees the security personnel at NIST who implement physical security policies, for example, while NIST manages access control technologies and other physical security countermeasures. This security structure violates best practice for security, which calls for centrally managing physical security assets and operations. Without a cohesive organizational structure, it seems inevitable that gaps in security will continue to emerge, and the management of NIST's security will be inefficient and potentially ineffective in confronting threats to the Agency and its employees.

GAO, in its review, pointed out further problems with NIST security management that we will hear more about today. It is worth noting that the GAO's security review also found that NIST's

leadership has made a positive commitment to improving security and that 75 percent of NIST staff surveyed by GAO believed that NIST's leadership places a "great" or "very great" importance on security issues. This commitment to security is encouraging, but there is much room for concrete improvements. I expect the leadership at the Department of Commerce and NIST to work together to fully and quickly address the issues outlined in the GAO report.

I believe NIST is a vital federal science agency, and that is why I am concerned about the physical security issues highlighted in the GAO report. The science and technology research and programs carried out at NIST helps U.S. businesses grow, it strengthens the U.S. economy, and it expands our scientific and technical knowledge. The public, and Congress, expect NIST to not only protect their vital resources, and in some cases hazardous materials, from potential threats, but also to protect NIST's employees, visiting scientists and others from physical security risks. I would also point out that the Acting Director of NIST, Dr. Kent Rochford, only stepped into this role in January. I am glad you are here today Dr. Rochford to tell us how you plan to address these important issues moving forward.

Finally, I would like to note my disappointment with the Department of Commerce and NIST for their late submittal of their testimony for today's hearing. They submitted their testimony less than 24 hours ago, well after the 48 hour deadline. Additionally, NIST and Commerce submitted joint written testimony that was unexpected and surprised the Science Committee Majority and Minority. Perhaps Dr. Rochford and Ms. Casias can explain this in their testimony.

Thank you Chairman LaHood for calling this hearing. Thank you to all of our witnesses, particularly to the GAO's Seto Bagdoyan and his team, for its work on this issue. I look forward to hearing from each of our witnesses.

I yield back.

Chairman LAHOOD. Thank you, Mr. Beyer.

I now recognize the Chairwoman of the Research and Technology Subcommittee, Ms. Comstock, for her opening statement.

Mrs. COMSTOCK. Thank you, Mr. Chairman.

This Committee has a strong record of bipartisan support for the National Institute of Standards and Technology (NIST). NIST promotes U.S. innovation and competitiveness by advancing measurement science, standards, and technology.

Today, we will be discussing a handful of dangerous physical security breaches at NIST's two campuses in Gaithersburg, Maryland, and Boulder, Colorado. Unfortunately, this isn't the first hearing we have held on this subject, but we certainly hope that it will be the last and certainly hope we can identify how can we move forward on improvements.

Lack of security at NIST facilities is a direct, serious threat to the safety and well-being of thousands of federal workers, a steady stream of scientists and technologists who visit NIST facilities every day, and sizable populations of people who live and work near the NIST facilities.

NIST's campus security has been a growing concern of the Committee since the July 2015 explosion at NIST's Gaithersburg facility, which revealed a NIST police officer, a former acting chief of NIST police, was operating an illegal meth lab at a NIST building. This event was the catalyst for bringing to light other security breaches at the Gaithersburg campus. Not quite one year later, in April 2016, another, no less serious incident occurred in Boulder, Colorado. A man without identification walked onto the NIST campus and was able to enter a building and laboratory where hazardous chemicals were stored. Fortunately, this man wasn't intent on playing around with laboratory chemicals and equipment or causing other damage. He instead roamed about the building and made himself at home.

Fortunately, the meth lab at the NIST Gaithersburg campus exploded on a weekend evening, not that it's fortunate but at least it was a weekend when NIST staff and visitors weren't there. But luck does run out.

We are going to hear this morning from NIST and Department of Commerce witnesses who will describe steps that were taken to shore up physical security after these two incidents. We are also going to hear about the results of a GAO investigation conducted at our Committee's request, which reveals that there are still serious, unaddressed security problems at NIST's Maryland and Colorado facilities. What we are going to hear today from GAO is serious enough that the Department may not allow certain details to be included in the public record.

NIST must learn from its past and do its best to ensure proper security is implemented, and obviously we all here in the Committee want to make sure that's the case. This is critical for the safety of NIST campuses, its employees, visitors, and the surrounding community.

It is also important not to jeopardize NIST's mission to promote U.S. innovation and industrial competitiveness. Physical insecurity at NIST's two locations obviously jeopardizes the important work done by the agency. Even more important, what seems to be huge,

unfixed holes in security threaten the safety and well-being of approximately 3,000 NIST employees, 3,500 visiting professionals government agencies. The safety of our people should be the number-one concern. Safety is certainly the number-one concern for this Committee.

I trust this hearing today will mark the end of the measures that haven't been successful and the beginning of swift, uncompromising action by NIST and the Department of Commerce.

Thank you.

[The prepared statement of Mrs. Comstock follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
October 11, 2017

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement from Chairwoman Barbara Comstock (R-Va.)

NIST's Physical Security Vulnerabilities: A GAO Undercover Review

Chairwoman Comstock: This Committee has a record of strong, bipartisan support for the National Institute of Standards and Technology (NIST). A non-regulatory agency within the Department of Commerce, NIST promotes U.S. innovation and competitiveness by advancing measurement science, standards, and technology.

NIST plays a very important role when it comes to constantly evolving cyber threats and technology by providing guidelines and standards to help reduce cyber risks to federal agencies and critical infrastructure. It is timely to note that October is National Cybersecurity Awareness Month.

Our subcommittee hears from NIST witnesses regularly on subjects like cybersecurity and boosting innovation and international competitiveness among American manufacturers.

Today, however, we will be discussing a handful of dangerous physical security breaches at NIST's two campuses in Gaithersburg, Maryland and Boulder, Colorado. This is not the first hearing we have held on this subject, but we all hope that it is the last.

Lack of security at NIST facilities is a direct, serious threat to the safety and well-being of thousands of federal workers, a steady stream of scientists and technologists who visit NIST facilities every day, and sizable populations of people who live and work near the NIST facilities.

NIST's campus security has been a growing concern of this Committee since the July 2015 explosion at NIST's Gaithersburg facility which revealed a NIST police officer – a former acting chief of NIST police – was operating an illegal meth lab at a NIST building. This event was the catalyst for bringing to light other security issues at the Gaithersburg campus.

Not quite one year later, in April 2016, another, no less serious incident occurred at the NIST facilities in Boulder, Colorado. A man without identification walked onto the NIST campus and was able to enter a building and laboratory where hazardous chemicals were stored.

Luckily, this man wasn't intent on playing around with laboratory chemicals and equipment or causing other damage. He instead roamed about the building and made himself at home.

Luckily, the meth lab at the NIST Gaithersburg campus exploded on a weekend evening, when NIST staff and visitors weren't around.

But luck always runs out.

We are going to hear this morning from NIST and Department of Commerce witnesses who will describe steps that were taken to shore up physical security after these two incidents.

We are also going to hear about the results of a GAO investigation conducted at our Committee's request, which reveals that there are still serious, unaddressed security problems at NIST's Maryland and Colorado facilities.

What we are going to hear today from GAO is serious, serious enough that the Department may not allow certain details to be included in the public record.

NIST must learn from its past and do its best to ensure proper security is implemented. This is critical for the safety of NIST campuses, its employees, visitors, and the surrounding communities.

It is also important not to jeopardize NIST's mission to promote U.S. innovation and industrial competitiveness, which enhances economic security and improves quality of life.

Physical insecurity at NIST's two locations obviously jeopardizes the important work done by the agency. Even more important, what seems to be huge, unfixed holes in security at NIST facilities threatens the safety and well-being of approximately 3,000 NIST employees; 3,500 visiting professionals from industry, academia, and other government agencies; and hundreds of thousands of residents of nearby communities.

The safety of our people should be the number-one concern. Safety is certainly the number-one concern for this Committee.

I hope and trust that today's hearing marks the end of temporizing and halfway measures and the beginning of swift, uncompromising action by NIST and the Department of Commerce.

###

Chairman LAHOOD. Thank you, Chairwoman Comstock.

I now recognize the Ranking Member of the Research and Technology Subcommittee, Mr. Lipinski, for his opening statement.

Mr. LIPINSKI. I'll start by also thanking Chairman LaHood, Chairwoman Comstock, Chairman Smith for calling this hearing, and thank the witnesses for being here. I'll keep this brief as my colleagues have stated many of the issues and concerns that I also have.

The National Institute of Standards and Technology is a national treasure. I know of no other agency that has such a widespread impact with so modest a budget: Nobel Prize-winning research, leadership standards development benefiting every sector of our economy, acceleration of advanced manufacturing on U.S. shores, and improvement of cybersecurity in both the government and the private sector. NIST's leadership in measurement science and their work in cybersecurity and so many other important areas of technology is unimpeachable.

Today, however, we will learn in some detail about how NIST has not applied the same rigor and discipline to the physical security of its facilities. A new report from GAO, being released with this hearing, identifies several weaknesses in NIST's policies and procedures for physical security. The GAO report further discusses the challenges caused by the fragmentation of oversight of NIST security between NIST and its parent agency, the Department of Commerce. GAO makes a number of recommendations to both NIST and Commerce on how to improve physical security on the two NIST campuses in Gaithersburg, Maryland, and Boulder, Colorado. Those recommendations are not prescriptive; rather they lay out or reference a clear process for the development of action plans and timetables to address each identified weakness in current policies and procedures.

While it is premature to ask NIST and Commerce for detailed plans, I expect to hear from them today how they plan to proceed in addressing each of GAO's recommendations, and what steps they have already taken.

I want to thank each of the witnesses for being here this morning. This hearing is not as fun for anyone as the science-and-technology-focused hearings that we're more used to in the Research and Technology Subcommittee, but it is certainly no less important. I take our oversight responsibilities seriously, and I believe the agencies before us take their security seriously. I look forward to learning more about the agencies' security plans going forward.

I yield back the balance of my time.

[The prepared statement of Mr. Lipinski follows:]

OPENING STATEMENT
Ranking Member Daniel Lipinski (D-IL)
of the Subcommittee on Research and Technology

House Committee on Science, Space and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
NIST's Physical Security Vulnerabilities: A GAO Undercover Review
October 11, 2017

Thank you Chairman LaHood and Chairwoman Comstock for calling this hearing, and thank you to the witnesses for being here this morning.

I will keep this brief. The National Institute of Standards and Technology is a national treasure. From Nobel prize-winning research, to their leadership in standards development benefiting U.S. businesses across every sector of our economy, to their role in accelerating advanced manufacturing on U.S. shores, to their central role in improving cybersecurity in both the government and the private sector, I know of no other agency that has such a big and widespread impact with such a relatively small budget. NIST's leadership in measurement science and their work in cybersecurity and so many other important areas of technology is unimpeachable.

Today, however, we will learn in some detail about how NIST has not applied the same rigor and discipline to the physical security of its facilities. A new report from GAO, being released with this hearing, identifies several weaknesses in NIST's policies and procedures for physical security. The GAO report further discusses the challenges caused by the fragmentation of oversight of NIST security between NIST and its parent agency, the Department of Commerce.

GAO makes a number of recommendations to both NIST and Commerce on how to improve physical security on the two NIST campuses in Gaithersburg, MD and Boulder, CO. Those recommendations are not prescriptive; rather they lay out or reference a clear process for the development of action plans and timetables to address each identified weakness in current policies and procedures. While it is premature to ask NIST and Commerce for detailed plans, I certainly expect to hear from them today how they plan to proceed in addressing each of GAO's recommendations, and what steps they have already taken.

I want to thank each of the witnesses for being here this morning. This hearing isn't as fun for anyone as the science and technology focused hearings we're more used to in the Research and Technology Subcommittee, but it is no less important. I take our oversight responsibilities seriously, and I believe the agencies before us take their security seriously. I look forward to learning more about the agencies' security plans going forward.

I yield back the balance of my time.

Chairman LAHOOD. Thank you, Mr. Lipinski.

I now recognize the Chairman of the full Committee, Mr. Smith, for his opening statement.

Chairman SMITH. Thank you, Mr. Chairman.

The GAO conducted a comprehensive review of NIST's physical security posture. They used covert tactics and they found gaping holes in the agency's ability to protect their campuses. Undercover agents succeeded in breaching numerous checkpoints.

Today, I want to thank the GAO for their work. Their findings are alarming and confirmed our worst suspicions: NIST campuses are sieves.

On July 22, 2015, this Committee launched an investigation of NIST's security in the wake of chemical—of a chemical explosion and fire at the Gaithersburg, Maryland, campus. On July 18, 2015, the acting chief of the police services group, or "PSG," attempted to manufacture the illegal drug meth in one of NIST vacant laboratories. The local Gaithersburg, Maryland, police and fire departments responded to the scene and began a criminal investigation.

On January 7, 2016, this high-ranking PSG officer was sentenced to three and a half years in jail for manufacturing meth. Slowly we learned this was only the tip of the iceberg.

According to a July 2016 Department of Commerce Office of Inspector General's report, the very officer who caused the explosion on NIST's campus also had committed time and attendance fraud by claiming hours that he did not actually work. He was not the only officer engaged in this misconduct.

The final straw for the Committee was the April 2016 incident in Boulder, Colorado, where an unknown individual was found wandering in a NIST building. After this incident, we contacted GAO and asked them to investigate. While law enforcement personnel has stepped in and handled many of these incidents, and the GAO has disclosed their findings to the Department and NIST, I'm not convinced that NIST will actually achieve the necessary goal: a secure NIST compound at Gaithersburg and Boulder.

GAO, as I understand it, remains concerned that the Police Services Group and the security structure within NIST has not received proper scrutiny, a concern that is bolstered by the revelation that GAO agents successfully penetrated NIST campuses in 15 out of 15 attempts during their covert vulnerability testing. By the way, that is just incredible: 15 out of 15. Not much security there.

Now we have a new Administration in place, a pending nominee for NIST Director, and GAO's recommendations, I urge NIST and the Department to work together for comprehensive security reform.

Thank you, Mr. Chairman. I'll yield back.

[The prepared statement of Chairman Smith follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
October 11, 2017

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement from Chairman Lamar Smith (R-Texas)

NIST's Physical Security Vulnerabilities: A GAO Undercover Review

Chairman Smith: Thank you, Mr. Chairman. The GAO conducted a comprehensive review of NIST's physical security posture. They used covert tactics and they found gaping holes in the agency's ability to protect their campuses. Undercover agents succeeded in breaching numerous checkpoints.

Today, I want to thank GAO for their work. Their findings are alarming and confirmed our worst suspicions. NIST's campuses are sieves.

Let me remind everyone why we requested this GAO review.

On July 22, 2015, this Committee launched an investigation of NIST's security in the wake of a chemical explosion and fire at the Gaithersburg, Maryland, campus.

On July 18, 2015, the acting chief of the police services group or "PSG" attempted to manufacture the illegal drug methamphetamine in one of NIST's vacant laboratories. The local Gaithersburg, Maryland, police and fire departments responded to the scene and began a criminal investigation.

On January 7, 2016, this high-ranking PSG officer was sentenced to three and a half years in jail for manufacturing meth. Slowly we learned this was only the tip of the iceberg.

NIST personnel and the press shared anecdotes with the Committee that painted a dire picture of the security posture at both NIST campuses – Gaithersburg and Boulder, Colorado.

Some of these anecdotes were clearly workplace grudges; others were serious revelations of a culture of waste, fraud, and abuse pervasive amongst the Police Services Group.

According to a July 2016 Department of Commerce Office of Inspector General's report, the very officer who caused the explosion on NIST's campus also had committed time and attendance fraud by claiming hours that he did not actually work. He was not the only officer engaged in this misconduct.

The final straw for the Committee was the April 2016 incident in Boulder, Colorado, where an unknown individual was found wandering in a NIST building. After this incident, we contacted GAO and asked them to investigate.

While law enforcement personnel has stepped in and handled many of these incidents and the GAO has disclosed their findings to the Department and NIST, I am not convinced that NIST will achieve the necessary goal – a secure NIST compound at Gaithersburg and Boulder.

GAO, as I understand it, remains concerned that the Police Services Group and the security structure within NIST has not received proper scrutiny. A concern that is bolstered by the revelation that GAO agents successfully penetrated NIST campuses in 15 out of 15 attempts during their covert vulnerability testing.

Now that we have a new administration in place, a pending nominee for NIST Director, and GAO's recommendations, I urge NIST and the Department to work together for comprehensive security reform.

###

Chairman LAHOOD. Thank you, Chairman Smith.

I now yield to the Ranking Member of the full Committee, Ms. Johnson, for her opening statement.

Ms. JOHNSON. Thank you, Mr. Chairman.

Thank you very much, Mr. Chairman, and good morning. Welcome to our witnesses. I'd like to thank you and Chairman Comstock for holding this important hearing on the state of physical security at the National Institute of Standards and Technology (NIST).

NIST has had a number of serious problems with physical security in recent years. A rogue NIST police officer injured himself and damaged a NIST building in Gaithersburg while attempting to manufacture methamphetamines.

Additionally, there was a troubling incident of an unauthorized individual wandering around a supposedly secure building at the NIST Boulder campus.

These events spurred the Department of Commerce and NIST to review NIST's security practices and attempt to improve physical security at the NIST facilities. NIST requested independent assessments and developed an Action Plan based on those assessments.

Under the current Acting Director, Dr. Rochford, NIST has continued to focus on improving its security culture. While there may have been improvements to NIST's security culture, there appears to be plenty of room for additional improvements.

We learned from GAO's just-released report that the GAO agents were recently able to gain unauthorized access to areas of both the Gaithersburg, Maryland, and Boulder, Colorado, NIST campuses. It is particularly troubling that GAO's efforts were so successful even after NIST had taken steps to improve security. I look forward to hearing today from Acting Director Rochford about how NIST plans to respond to the GAO recommendations, including specific corrective actions and approximate timelines for improving and implementing those actions. I look forward to hearing from Ms. Casias about the Department of Commerce's plan to address the bifurcated organizational structure of NIST physical security programs. I would also like to know what actions the Department of Commerce plans to take to ensure NIST security services operate at maximum effectiveness.

The protection of federal facilities, employees, contractors, and guests is of the utmost concern to me and this Committee. NIST specifically has valuable research and technology that must be protected as well. I look forward to hearing from our witnesses about how NIST security services can better meet its mission.

I thank you, and yield back.

[The prepared statement of Ms. Johnson follows:]

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
"NIST's Physical Security Vulnerabilities: A GAO Undercover Review"
October 11, 2017

Good morning and welcome to our witnesses. Thank you to Chairman LaHood and Chairman Comstock for holding this important hearing on the state of physical security at the National Institute of Standards and Technology (NIST).

NIST has had a number of serious problems with physical security in recent years. A rogue NIST police officer injured himself and damaged a NIST building in Gaithersburg while attempting to manufacture methamphetamine. Additionally, there was a troubling incident of an unauthorized individual wandering around a supposedly secure building at the NIST Boulder campus. These events spurred the Department of Commerce and NIST to review NIST's security practices and attempt to improve physical security at NIST facilities. NIST requested independent assessments and developed an Action Plan based on the assessments. Under the current Acting Director, Dr. Rochford, NIST has continued to focus on improving its security culture.

While there may have been improvements to NIST's security culture, there appears to be plenty of room for additional improvement. We learned from GAO's just-released report that GAO agents were recently able to gain unauthorized access to areas of both the Gaithersburg, Maryland and Boulder, Colorado NIST campuses. It is particularly troubling that GAO's efforts were so successful even after NIST had taken steps to improve security.

I look forward to hearing today from Acting Director Rochford about how NIST plans to respond to the GAO recommendations, including specific corrective actions and an approximate timeline for implementing those actions. I look forward to hearing from Ms. Casias about the Department of Commerce's plans to address the bifurcated organizational structure of NIST physical security programs. I would also like to know what actions the Department of Commerce plans to take to ensure NIST security services operate at maximum effectiveness.

The protection of federal facilities, employees, contractors, and guests is of the utmost concern to me and this Committee. NIST specifically has valuable research and technology that must be protected as well. I look forward to hearing from our witnesses about how NIST security services can better meet its mission.

Thank you. I yield the balance of my time.

Chairman LAHOOD. Thank you, Ms. Johnson.

Let me now introduce our witnesses. Our first witness today is Ms. Lisa Casias, Deputy Assistant Secretary for Administration at the Department of Commerce. She previously served as the Deputy Chief Financial Officer and Director for Financial Management at the Department. Ms. Casias received her bachelor's of business administration in public accounting from Pace University.

Our second witness today is Dr. Kent Rochford, Acting Under Secretary of Commerce for Standards and Technology, and Acting Director of the National Institute of Standards and Technology (NIST). He previously served as the Director of NIST Boulder Labs and Communications Technology Laboratory headquartered in Boulder, Colorado. Dr. Rochford received his bachelor's degree in electrical engineering at Arizona State University, his MBA from the University of Colorado, and his Ph.D. in optical sciences from the University of Arizona.

Our third witness is Mr. Seto Bagdoyan, Director of Forensic Audits at the U.S. Government Office—Accountability Office (GAO). Mr. Bagdoyan has previously served as the GAO Acting Director for Strategic Issues and as the Assistant Director for Congressional Relations at GAO. Mr. Bagdoyan received his bachelor's degree in international relations and economics from Claremont McKenna College and his MBA in strategy from Pepperdine University.

I now recognize Ms. Casias for five minutes to present her testimony.

TESTIMONY OF MS. LISA CASIAS,
DEPUTY ASSISTANT SECRETARY
FOR ADMINISTRATION AT
U.S. DEPARTMENT OF COMMERCE

Ms. CASIAS. Thank you, Chairman LaHood, Ranking Member Beyer, Chairman Comstock, Ranking Member Lipinski, and distinguished members of the Subcommittees.

I am Lisa Casias, the Deputy Assistant Secretary for Administration at the U.S. Department of Commerce. In this role, I oversee the Department's Office of Security and its functions and personnel. I appreciate the opportunity to appear before you today to discuss the Department's response to the Government Accountability Office report titled "Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges."

Let me first thank GAO for its important work, which we will use to help strengthen security at NIST. I want the Committee to know that the Department of Commerce shares the GAO's and this Committee's concerns about physical security at NIST. The Department is proud of NIST's mission to promote U.S. innovation and industrial competitiveness through advancing measurement science, standards, and technologies in ways that enhance economic security and improve our quality of life.

However, our highest priority is the safety of all of our staff, guest workers, and visitors. We have carefully reviewed the draft report, and I can tell you that the findings revealed shortcomings that are absolutely unacceptable, and I know that Dr. Rochford agrees. We take the GAO's findings seriously, and both the Department and NIST have agreed with all of the recommendations set

forth in the report. NIST and the Department have already taken a number of steps to address the concerns raised in the report, and we are together planning more actions in the near and long term to close the gaps in security identified in the report.

For example, the Department's Office of Security has already implemented a requirement that all security specialists conducting facility security assessments be certified in Interagency Security Committee Risk Management Process, or "RMP standard." To date, 19 of our security specialist staff have successfully completed the ISC's RMP standard training and all security specialists will be trained in early fiscal year 2018. We have also scheduled new facility security assessments using those trained personnel at both campuses this fiscal year.

Additionally, OSY has completed a draft chapter for the Department's Manual for Security Policies and Procedures that will align with the Department's Risk Management Plan with the ISC's RMP standard. This chapter is currently in the review process within the Department. In addition to aligning the Department's Risk Management Plan with ISC's RMP standard, this update incorporates all the recommended elements from the GAO report related to campus facility Security Committee's risk decision documentation and alternative countermeasure recommendations.

We are also, as the GAO has recommended, reviewing the security structure at NIST. This review involves all aspects of the relationship between OSY and NIST related to personnel assets and security, and as part of a coordinated effort between the Department and NIST to determine the best approach. While there is no one-size-fits-all standard, we are reviewing all options available to us. These are only a few of the actions we have taken and are taking to ensure our campuses and facilities are secure and safe for our employees, guests, and others.

I wanted to reiterate my appreciation to GAO for their thoughtful and thorough report. The Secretary and the Department are committed to ensuring that our actions in response to it are appropriate, effective, and correct. The security and safety of all of NIST's and the Department's employees are of paramount importance to all of us.

Thank you for this opportunity to address the report, and I look forward to answering your questions.

[The prepared statement of Ms. Casias and Dr. Kent Rochford follows:]

Joint Statement for the Record

Lisa Casias
Deputy Assistant Secretary for Administration
U.S. Department of Commerce

Dr. Kent Rochford
Acting Undersecretary for Standards and Technology and Director
National Institute of Standards and Technology
U.S. Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight
and
Subcommittee on Research and Technology

U.S. Department of Commerce and National Institute of Standards and Technology Response to the Government Accountability Office's Report Entitled: *"Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges"*

October 11, 2017

Thank you Chairman LaHood, Ranking Member Beyer, Chairman Comstock, Ranking Member Lipinski, and distinguished members of the Subcommittees. We appreciate the opportunity to appear before you today to discuss the Department of Commerce's response to the recently released report by the Government Accountability Office (GAO) entitled: *"Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges."*

The National Institute of Standards and Technology (NIST)'s programs focus on national priorities from advanced manufacturing and the digital economy to precision metrology, quantum science, biosciences, and more. NIST's overall mission is to promote U.S. innovation and industrial competitiveness. NIST does this by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

As this Committee knows, the world-class research conducted at NIST needs world-class facilities to accomplish the NIST mission, but just as important, NIST needs robust, consistent adherence to standards for physical security to ensure that personnel are working in a safe environment and that our assets are protected. We are committed to bringing together all necessary Department resources to achieve that goal.

We welcome the Subcommittees' support of the Department's efforts to continue to improve overall security. The Department continues to take steps to improve the physical security at NIST and throughout the Department, and intends to fully implement the recommendations contained in the GAO report. Specifically, today we will discuss where we are in improving the security culture at both NIST campuses and across the Department, and the steps we have taken to ensure successful implementation of the report's recommendations.

The Office of the Assistant Secretary for Administration (ASA) oversees the Office of Security (OSY). The Secretary of Commerce has delegated authority to OSY to manage and implement all security, emergency management, and threat investigations across the Department and its 13 bureaus and operating units. The OSY's mission is to protect personnel, facilities, and information by collaborating with key leaders, decision-makers, and stakeholders across all of the Department's bureaus and operating units to effectively mitigate security risks throughout the Department.

Responsibility for security does not rest solely with OSY. The head of each operating unit or bureau is responsible for ensuring the security of the personnel, facilities, property, information and assets of their respective organizations in accordance with applicable laws, regulations, Executive Orders, and directives. The Director of Security is responsible for advising and assisting heads of operating units. Thus, NIST's Director shares with OSY the role of protecting the Department's personnel, mission, information, and infrastructure at NIST.

We are committed to a comprehensive assessment of the roles and responsibilities between OSY and NIST at NIST's two campuses, in Gaithersburg, MD, and Boulder, CO, as recommended in the GAO report. Currently, OSY is charged with delivering integrated law enforcement and security services and protection, while NIST is responsible for ensuring the physical security of the buildings. In practice, this means that NIST has primary responsibility for providing and

maintaining electronic locks, surveillance devices, and alarms at NIST's campuses. NIST also is responsible for establishing local campus security procedures, and the maintenance and management of the physical security systems such as access control systems, intrusion detection systems, identification badging, and other security and safety systems designed to protect NIST assets.

In turn, OSY provides the security personnel to monitor security cameras, undertake routine patrols of NIST's campuses and buildings, and provide emergency assistance. It also oversees a contract guard force that staff entry points to the campuses.

OSY manages upwards of 75 security personnel at NIST, utilizing a mix of Police Services Group (PSG) Officers and contract Protective Security Officers (PSO), along with oversight and support staff. The PSG and guard contract delegations were transferred to OSY in November 2015. Pursuant to section 113 of the American Innovation and Competitiveness Act, OSY employs a Director for Security at NIST who supervises the PSG and contract guards at NIST.

NIST takes its responsibility to ensure the physical security of NIST's two campuses very seriously. NIST is working with OSY to strengthen the security culture at NIST, which the GAO notes has already had some success, though there is still more work to be done.

GAO Report

The GAO, at the request of this Committee and the Senate Committee on Commerce, Science, and Transportation, undertook a comprehensive review of the physical security of NIST's campuses in Gaithersburg and Boulder. We appreciate the GAO's efforts as it provides us with important information and an additional perspective as we work to strengthen security across the Department and at NIST.

The GAO's report made four recommendations: two directed primarily to OSY, and two directed primarily to NIST, although both OSY and NIST recognize that we must continue to work together to strengthen security at the campuses. We agree with the GAO's recommendations, and have taken a number of steps to implement them. So far, we have:

- Implemented, through OSY, the requirement that all Security Specialists conducting Facility Security Assessments be trained and certified through the Interagency Security Committee (ISC) Risk Management Process (RMP) in FY17. Beginning in FY18, all DOC Facility Security Assessments will be conducted in accordance with the ISC RMP. In implementing these activities, the Department's Manual for Security Policies and Procedures has been aligned with the ISC RMP. This chapter is currently in the Department's internal clearance process. This update also incorporates all recommended elements from the GAO report related to campus Facility Security Committees, risk decision documentation, and alternative countermeasure recommendations.

- Increased oversight, testing and inspection, both announced and unannounced, of Protective Security Officers. Additionally, Protective Security Officers have also been retrained to reinforce the security posture and effectiveness of security access points at various Department campuses and facilities.

- Through OSY, continued implementation of "Security Awareness Day" across the Department, and specifically at NIST, to increase employee awareness of security, safety and emergency responsibilities, policies, procedures and programs. In fact, the NIST Gaithersburg campus held its Security Awareness Day on October 10 and Boulder campus is scheduled to hold its Security Awareness Day on October 19.

- Dedication by NIST of approximately $4M for physical security programs and systems enhancements, reflecting our commitment to the physical security of NIST campuses, and the ability of NIST personnel to work in a safe environment.

- Developed in 2016 NIST's internal Security Policy. As the GAO report acknowledges, this action and others demonstrated "leadership's commitment to transforming NIST's security culture." The Security Policy is intended to ensure the security of NIST personnel, buildings, and other plant facilities, equipment, property, and assets.

- Established NIST's Security Advisory Board (SAB) in January 2017, which the GAO report observed "affirms the commitment of NIST management to establishing and maintaining a comprehensive, effective, and efficient agency-wide approach to physical security at NIST."

- Initiating the addition of a security element to all NIST employees' performance plans, ensuring that security is afforded the same high level of importance in one's job performance as other elements. This effort and others will drive a culture of change with respect to security.

- Already conducting a "Security Sprint" or a deep dive into NIST's work to prioritize its security needs, applying many of the ISC RMP principles, and developing action items necessary to address those needs. NIST has prioritized the actions and is currently implementing many of these actions. As recommended by GAO, NIST and the Department are incorporating elements of key practices of risk management, as well as interim milestones, into the implementation of the Security Sprint Action Plans.

Finally, the GAO report recommends the Department assess the current security organizational structure between OSY and NIST. The report encourages us "to identify the most effective and feasible approach to physical security at NIST." While each of these entities currently has specific, non-duplicative responsibilities, we recognize that there might be alternative organizational structures that may more effectively promote security. For that reason, the Department is undertaking a comprehensive, holistic assessment of the NIST physical security

organization as recommended by the GAO and will take a fresh look at the most appropriate and effective roles and responsibilities for OSY and NIST to best manage our security challenges.

Secretary Ross is committed to ensuring safety and security across the Department of Commerce. We appreciate the Subcommittees' interest in the Department's ongoing work to improve the physical security at NIST's campuses, and we welcome your questions.

Lisa Casias
Deputy Assistant Secretary for Administration
U.S. Department of Commerce

Lisa Casias was named the Deputy Assistant Secretary for Administration (DASA) within the Office of the Chief Financial Officer and Assistant Secretary for Administration (OCFO/ASA) effective March 6, 2016. In this role, she is responsible for a broad range of department-wide functions, including acquisition management, privacy and open government, facilities and environmental quality, civil rights, human resources management, and security.

Immediately preceding her assignment as the DASA, Ms. Casias served as the Deputy Chief Financial Officer and Director for Financial Management. As Deputy CFO, she was responsible for financial management and accounting throughout the Department; for preparation of the Department's annual consolidated financial statements; for development and implementation of a Department-wide integrated financial system; and for providing policy, oversight, and guidance for personal property, fleet management services, and travel and conference-related expenditures.

Ms. Casias joined the Department in November 1991 as the Deputy Assistant Inspector General for Financial Statements Audits in the Office of the Inspector General before moving to the OCFO/ASA, Office of Financial Management, as the Deputy Director for Financial Policy.

Prior to her federal government career, Ms. Casias was an audit supervisor with an international public accounting firm.

Ms. Casias is a Certified Public Accountant and holds her BBA in public accounting from Pace University. She is the recipient of the 2009 Presidential Distinguished Rank Award and has served as the National President of the Association of Government Accountants.

Kent Rochford

Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Dr. Rochford is Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director. As principal NIST deputy director, Dr. Rochford assumed this role on January 4, 2017, following the retirement of previous director Willie E. May. As NIST Acting Director, Dr. Rochford provides high-level oversight and direction for NIST.

Dr. Rochford's current permanent position is NIST's Associate Director for Laboratory Programs (ADLP). As ADLP, he provides direction and operational guidance for NIST's scientific and technical mission-focused laboratory programs and serves as principal deputy to the Under Secretary of Commerce for Standards and Technology and NIST director, among other duties.

Dr. Rochford was formerly director of NIST-Boulder Labs and the Communications Technology Laboratory (CTL), also headquartered in Boulder, Colo. He was responsible for the creation of the CTL, which focuses on measurement science to assist first responder communications, spectrum sharing and advanced communications technologies, and support for the National Advanced Spectrum and Communications Test Network (NASCTN).

Previously, Dr. Rochford served as chief of both the Quantum Electronics and Photonics and Optoelectronics Divisions at NIST, as well as acting director of the Electronics and Electrical Engineering Laboratory.

Apart from NIST, Dr. Rochford served as senior director for Sharp Laboratories of America's Material and Device Applications laboratory and managed systems R&D at YAFO Networks, a fiber-optic communications start-up.

Dr. Rochford received his Ph.D. in optical sciences from the University of Arizona, Bachelor of Science degree in electrical engineering at Arizona State University, and an MBA from the University of Colorado.

Chairman LAHOOD. Thank you.
Dr. Rochford.

TESTIMONY OF DR. KENT ROCHFORD, ACTING UNDER SECRETARY OF COMMERCE FOR STANDARDS AND TECHNOLOGY AND ACTING DIRECTOR AT NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. ROCHFORD. Chairman LaHood, Ranking Member Beyer, Chairwoman Comstock, Ranking Member Lipinski, and members of the Subcommittee, I'm Kent Rochford, the Acting Under Secretary of Commerce for Standards and Technology, and the Acting Director of the National Institute of Standards and Technology, or "NIST." Thank you for the opportunity to appear before you today to discuss NIST's and the Department's response to the recently released report by the GAO on physical security at NIST.

I share the Subcommittees' concerns about physical security at our campuses, and I thank you for your comments. I also appreciate your kind words about our programmatic successes, so thank you for that.

I also appreciate the Subcommittees' support of NIST's efforts to improve our security practices and to fully implement the recommendations in the report, with which we agree. NIST and the Department of Commerce are working to foster a positive security culture at both of our campuses, and the written testimony outlines the steps that we've already taken or plan to take to improve NIST's security posture and ensure the successful implementation of the report's recommendations.

The world-class research conducted at NIST needs world-class facilities to conduct that mission, but just as important, NIST needs robust, consistent adherence to standards for safety and physical security to ensure our people work in a safe environment and that our assets are protected. I am committed to working with our partners at the Department to achieve this goal.

As the Acting Director, it's my job to ensure the safety and security of our personnel, facilities, property, information, and assets, and I take that responsibility very seriously, and that's why we are working together with the Department's Office of Security to ensure the security of NIST staff, that my co-workers, can work safely and securely, and for establishing local campus security procedures designed to protect NIST assets.

Moreover, NIST continues to work with the Department's Office of Security to strengthen the security culture at NIST. The GAO notes that we have already had some success but we also acknowledge there is still more work to be done. The GAO's report made four recommendations. NIST and the Department agree with the full extent of these recommendations.

Upon becoming Acting Director in January of this year, one of my first actions was to build on the foundational work started by Dr. May and the Department's Office of Security and prioritize our activities through a Security Sprint. I considered it critically important to take the existing information we had, the knowledge we'd

gained during the previous year, and prioritize our activities to move forward with implementation plans.

The GAO pointed out the importance of improved communication with staff concerning physical security requirements, and what should be expected of each employee. NIST agrees, and we have taken steps to improve our internal communications. We've developed an improved set of security requirements designed to provide an unambiguous understanding of the security responsibilities of all individuals who work at NIST.

Last month, I met with senior NIST leadership and the Department's Office of Security to ensure that these requirements and expectations were fully understood. This afternoon, we will meet with the full complement of NIST management and supervisors to ensure that these security requirements and expectations are fully understood by all NIST leaders. And following that, I will hold all-staff meetings to roll out these responsibilities and expectations and training requirements that all staff must meet.

I also initiated the inclusion of a security element and all-employee performance plans for this fiscal year, ensuring that security is afforded the same high level of importance in one's job performance as other elements. My intent is to work with OSY to drive a change towards a positive security culture. These efforts and others will help drive that change.

Mr. Chairman, NIST has a history of tackling tough problems from research challenges like developing the world's most atomic clock to internal challenges such as addressing our safety culture. The dedicated people at NIST have committed themselves to working toward a common goal of achieving NIST's mission. We along with OSY are now in the midst of such an effort for physical security. I appreciate the Subcommittees' interest in our ongoing work to improve the physical security of our campuses, and I welcome your questions. Thank you.

Chairman LAHOOD. Thank you, Dr. Rochford.

Now we'll move to our third witness, Mr. Bagdoyan.

TESTIMONY OF MR. SETO BAGDOYEN, DIRECTOR, AUDIT SERVICES AT U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. BAGDOYAN. Thank you, Mr. Chairman. Chairman Smith, Ranking Member Johnson, Chairman LaHood, Chairwoman Comstock, Ranking Members Lipinski and Beyer, and members of the Subcommittees, I'm pleased to appear before you today to discuss GAO's October 2017 report on NIST's physical security program. In recent years, incidents at each of its campuses in Gaithersburg and Boulder have raised questions about security vulnerabilities and NIST's ability to secure its facilities and the human, physical, and intellectual capital assets.

In fiscal year 2017, NIST spent over $600 million on its campus laboratories that perform vital work in measurements, calibrations, and quality assurance techniques that help underpin much of U.S. commerce. Accordingly, this morning I'll highlight three of our principal takeaways regarding NIST's security at its campuses.

First, we found that efforts to transform the physical security program at NIST have incorporated some key practices, particu-

larly with regard to leadership commitment to organizational change. For example, though assessments in 2015 found issues with NIST's security culture, we estimate that about 75 percent of personnel we recently surveyed believe that NIST leadership places great or very great importance on security issues. However, our agents gained unauthorized access to various areas at NIST campuses in Gaithersburg and Boulder. We can provide details about our unauthorized access efforts and certain survey results only during a closed session of this hearing.

Additionally, our survey results showed personnel awareness about security responsibilities varied, in part because of the limited effectiveness of NIST's security-related communication efforts. By incorporating elements of key practices including a comprehensive communications strategy, interim milestone dates to measure progress, and measures to assess effectiveness, NIST will be in a better position to address the security vulnerabilities caused by the varied levels of security awareness among employees.

Second, management of NIST's physical security program is split between Commerce and NIST. This is inconsistent with the federal Interagency Security Committee's physical security best practices, which encourage agencies to centrally manage physical security. Commerce is responsible for overseeing personnel who implement physical security policies while NIST manages physical security countermeasures such as access control technology leading to fragmentation in responsibilities.

Before implementing the current organizational structure in October of 2015, neither Commerce nor NIST assessed whether it was the most appropriate way to fulfill NIST's physical security responsibilities. Without evaluating management options, the current organizational structure may be creating unnecessary inefficiencies, thereby inhibiting the effectiveness of the security program overall.

Third, to help federal agencies protect and assess risks to their facilities, ISC developed a Risk Management Process standard, also known as the "RMP standard," with which federal agencies including Commerce generally must comply. Commerce and NIST most recently completed risk management steps for NIST campuses in 2015 and 2017 but we found that their efforts did not fully align with the standard. Neither Commerce nor NIST use the sound risk assessment methodology, fully documented key risk management decisions or appropriately involved stakeholders, partly because these requirements were not in existing policy.

Further, we found that Commerce and NIST had overlapping risk management activities potentially leading to unnecessary duplication. According to officials, Commerce and NIST are separately drafting new risk management policies without ensuring that one, these policies aligned with the RMP standard, and two, that NIST policy contains a formal mechanism to coordinate with Commerce future risk management activities may be limited in their usefulness and potentially duplicative.

In closing, I'd underscore that this is essential for Commerce and NIST to place a high policy and operational priority on deploying preventative security controls to help mitigate the vulnerabilities we identified. Otherwise, should these vulnerabilities be exploited, NIST's human, physical, and intellectual capital will remain at

risk. Fully and timely implementing our report's four recommendations in addition to any other actions Commerce and NIST are taking independently would be vital in this regard. To its credit, as both witnesses from Commerce have mentioned, the Department has agreed to implement all of our recommendations.

Chairman LaHood, Chairwoman Comstock, Chairman Smith, and Ranking Member Johnson, this concludes my remarks. I look forward to the Subcommittees' questions.

[The prepared statement of Mr. Bagdoyan follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittees on Oversight and Research and Technology, Committee on Science, Space, and Technology, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Wednesday, October 11, 2017

PHYSICAL SECURITY

NIST and Commerce Need to Complete Efforts to Address Challenges

Statement of Seto J. Bagdoyan, Director, Forensic Audits and Investigative Service

Chairman LaHood, Chairwoman Comstock, Ranking Members Beyer and Lipinski, and Members of the Subcommittees:

Thank you for the opportunity to discuss our work on the physical security program at the National Institute of Standards and Technology (NIST). NIST is responsible for providing the measurements, calibrations, and quality-assurance techniques that underpin commerce, technological progress, improved product reliability, and manufacturing processes in the United States. In 2017, NIST, located within the Department of Commerce (Commerce), employed approximately 3,500 federal personnel and hosted 4,000 associates, who include guest researchers and facility users, among others.

Recent incidents have raised questions about security vulnerabilities at NIST and the agency's ability to properly secure its physical facilities and assets. Specifically, in July 2015, a federal police officer at the NIST campus in Gaithersburg, Maryland, caused an explosion while attempting to illegally manufacture methamphetamine in a partially vacant laboratory building. In April 2016, an individual unaffiliated with NIST gained unauthorized access to a secured facility at NIST's Boulder, Colorado, campus and subsequently required medical attention. These incidents have also prompted efforts by NIST to transform its security program.

Commerce and NIST currently share responsibilities for ensuring the security of NIST facilities. Specifically, the Office of Security (OSY) within Commerce is responsible for overseeing NIST's Police Services Group (PSG) and contract guards, as well as personnel and information security.[1] NIST's Emergency Services Office manages physical security countermeasures, such as access control technology and closed-circuit televisions. Commerce is also responsible for protecting NIST facilities, assets, and employees from security threats or violent acts, in part by assessing risks to these facilities.

To help federal agencies protect and assess risks to their facilities, the federal Interagency Security Committee (ISC) developed a physical security standard, *The Risk Management Process for Federal Facilities*

[1]Pursuant to 15 U.S.C. § 278e(b), the Secretary of Commerce is authorized to undertake activities related to the care, maintenance, protection, repair, and alteration of NIST buildings and other plant facilities, equipment, and property.

(RMP Standard),[2] with which all federal executive-branch agencies, including Commerce, generally must comply.[3]

My remarks today are based on our report that is being released at this hearing.[4] This report is the public version of a sensitive report that was also issued in October 2017.[5] Specifically, this testimony discusses the extent to which (1) efforts to transform the physical security program at NIST incorporated key practices and addressed security vulnerabilities; (2) the organizational structure of the NIST physical security program reflects best practices; and (3) NIST's risk management process for physical security aligns with ISC standards and best practices.

For our reports, we employed several methods to develop our findings. We conducted a generalizable survey of 506 randomly selected NIST employees and associates to identify common themes related to perspectives about NIST's physical security program. We also conducted covert surveillance and nongeneralizable vulnerability testing at the Gaithersburg and Boulder campuses, and interviewed relevant Commerce and NIST officials. In addition, we compared OSY and NIST's risk management activities performed for both campuses in 2015 and 2017 to the RMP Standard. Additional information on our scope and methodology is available in our October 2017 reports. Our audit work for these reports was performed in accordance with generally accepted

[2]Interagency Security Committee, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (November 2016). This RMP Standard incorporates the following appendixes as separate documents: Appendix A: *The Design-Basis Threat Report (FOUO)*; Appendix B: *Countermeasures (FOUO)*; and Appendix C: *Child-Care Centers Level of Protection Template (FOUO)*.

[3]The ISC is chaired by the Department of Homeland Security (DHS) and comprises 60 member agencies. The ISC was created pursuant to Executive Order 12977, 60 Fed. Reg. 54411 (Oct. 19, 1995) and subsequently amended by Executive Order 13286, 68 Fed. Reg. 10619 (Feb. 28, 2003). The ISC is housed within DHS's National Protection and Programs Directorate, Office of Infrastructure Protection.

[4]GAO, *Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges*, GAO-18-95 (Washington, D.C.: Oct. 11, 2017).

[5]GAO, *Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges*, GAO-18-14SU (Washington, D.C.: Oct. 4, 2017). Commerce and DHS deemed some of the information in this report to be sensitive, which must be protected from public disclosure. Therefore, GAO-18-95 omits sensitive information about our investigative methods, as well as specific details regarding security measures, threats, and vulnerabilities, the release of which could pose unintended security risks. Although the information provided in GAO-18-95 is more limited, it addresses the same objectives as the sensitive report and uses the same methodology.

government auditing standards, and our related investigative work was done in accordance with investigative standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

In summary, we found that

- efforts to transform the physical security program at NIST incorporate some key practices but do not fully address security vulnerabilities;
- the organizational structure of NIST's physical security program does not fully reflect best practices, potentially inhibiting effectiveness; and
- OSY and NIST have taken some steps to align NIST's risk management process with ISC standards but could better coordinate future activities.

We made four recommendations to address these issues, and Commerce agreed with each of the recommendations.

Efforts to Transform the Physical Security Program at NIST Incorporate Some Key Practices but Do Not Fully Address Security Vulnerabilities

Since 2015, NIST and OSY's efforts to transform the physical security program at NIST have incorporated some key practices associated with effective organizational transformations but have not yet addressed others.[6] In particular, leadership has taken steps to improve organizational culture associated with physical security, such as by obtaining independent assessments, developing an Action Plan, and then initiating a Security Prioritization Sprint (Security Sprint). By taking these steps soon after the security incident at the Gaithersburg campus in July 2015, NIST leadership made a statement about the importance of change and demonstrated a commitment to making change, which are key practices associated with effective organizational transformation. For example, on the basis of our survey, we estimate that as of May 2017 about three-quarters of NIST scientific and technical employees believe

[6]We have previously identified key practices of successful large-scale organizational transformations, which include (1) ensuring top leadership drives the transformation; (2) establishing a coherent mission and integrated strategic goals to guide the transformation; (3) focusing on a key set of principles and priorities; (4) setting implementation goals and a timeline; and (5) establishing a communication strategy to create shared expectations and report related progress. We determined that some of the key practices identified in our prior work, such as changing the agency's overall performance management system, did not apply to our assessment, given the status of NIST's ongoing transformation of its physical security program. GAO, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2, 2003).

that NIST leadership places "great" or "very great importance" on physical security issues, suggesting that leadership has been successful at demonstrating its commitment to security through recent efforts.[7]

Although NIST leadership has taken some steps to transform the organizational culture related to physical security at NIST, these efforts have not fully addressed security vulnerabilities. We found that varied levels of staff awareness about security responsibilities created security vulnerabilities, partly due to the limited effectiveness of NIST's security-related communication efforts. We identified security vulnerabilities through our covert vulnerability testing, during which GAO agents gained unauthorized access to various areas of both NIST campuses.[8] We also identified security vulnerabilities through our survey results. For example, some NIST employees who are not required to complete security training reported having observed colleagues not following certain NIST security policies.[9] In contrast, NIST employees working in highly sensitive facilities, all of whom are required to complete additional mandatory security training, reported significantly fewer observations of colleagues not following NIST security policies. As part of its ongoing Security Sprint, NIST has begun to address these issues through action plans. However, these action plans do not incorporate key practices, such as establishing a communication strategy, interim milestone dates, and measures to assess effectiveness. By incorporating these practices, NIST will be better positioned to effectively address the security vulnerabilities caused by varied levels of security awareness among employees.

In our report released today, we recommend that the NIST Director incorporate elements of key practices into NIST's ongoing security efforts. Commerce agreed with this recommendation.

[7]We conducted a generalizable survey from March 17, 2017, through May 10, 2017. Our survey reflects the efforts of NIST leadership prior to the Security Sprint, because the initial phase of that effort was not completed until April 2017. During the time frame of the survey, NIST did not take any action related to the Security Sprint report.

[8]The findings from our covert vulnerability testing represent illustrative examples and are not generalizable.

[9]Details related to the specific scenarios and behaviors we asked about, as well as the associated survey results, are provided in the sensitive version of this report, GAO-18-14SU.

The Organizational Structure of NIST's Physical Security Program Does Not Fully Reflect Best Practices, Potentially Inhibiting Effectiveness

The organizational structure of NIST's physical security program does not fully reflect best practices, which encourage agencies to centrally manage physical security through a Director of Security or Chief Security Officer. Since 2015, responsibility for physical security at NIST has been split between OSY and NIST, and management of the program has been fragmented.[10] Many of OSY and NIST's responsibilities, however, must be integrated to effectively implement the physical security program. For example, NIST maintains the physical infrastructure required to secure campus perimeters, while the PSG and contract guards patrol and secure the campus. While the best practices indicate that the Director of Security is usually within an agency's internal security office, in the case of NIST, the 2017 American Innovation and Competitiveness Act requires OSY to directly manage the law-enforcement and site-security programs of NIST through an assigned Director of Security for NIST.[11]

Prior efforts by NIST, including the Security Sprint, have noted that the existing organizational structure limits the effectiveness of NIST's security program. However, neither OSY nor NIST evaluated the feasibility of other organizational options for NIST's physical security program before proposing to implement the current structure. Further, despite the findings of the Security Sprint and other assessments, there are no plans to assess whether the current structure is the most appropriate way to fulfill NIST's security requirements. An evaluation could provide the NIST Director and Congress with greater assurance that the current structure is the most effective and feasible approach to physical security at NIST, or identify whether a consolidated security structure centrally managed by OSY, which would comply with the American Innovation and Competitiveness Act requirements, might better suit NIST's security requirements. Without an evaluation, the structure, which has been in place since October 2015, will likely create unnecessary inefficiencies and competing priorities, and thereby inhibit the effectiveness of the physical security program overall, as well as ongoing efforts to improve the program.

[10]We have defined fragmentation as those circumstances in which more than one federal agency (or more than one organization within an agency) is involved in the same broad area of national need and opportunities exist to improve service delivery. GAO, *2017 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO-17-491SP (Washington, D.C.: Apr. 26, 2017).

[11]Pub. L. No. 114-329, § 113, 130 Stat. 2969 (Jan. 6, 2017).

In our report released today, we recommend that the Director of OSY, in coordination with the NIST Director, evaluate the effectiveness of the current security management structure. Commerce agreed with our recommendation.

OSY and NIST Have Taken Some Steps to Align NIST's Risk Management Process with ISC Standards but Could Better Coordinate Future Activities

OSY and NIST's most-recent risk management activities for physical security at NIST's campuses did not fully align with the RMP Standard.[12] Specifically, neither OSY nor NIST used sound risk assessment methodologies, fully documented key risk management decisions, or appropriately involved stakeholders when completing steps in the risk management process in 2015 and 2017. OSY is revising Commerce's department-wide security risk management policy and developing guidance, which could address some issues with OSY and NIST's recent efforts, such as issues with their risk assessment methodologies and documentation of key decisions. In addition, while the draft policy provided to us in July 2017 did not contain specific requirements associated with stakeholder involvement and ISC training, an OSY official stated that such requirements would be included in the final policy. If finalized and implemented as intended, these policy changes and guidance could directly address some of the issues we identified in OSY and NIST's risk management activities (see table 1).

Table 1: Extent to Which the Department of Commerce's (Commerce) Planned Risk Management Policy and Guidance Revisions Would Address Some Issues at the National Institute of Standards and Technology (NIST)

Issue area	2015 Risk management activities	2017 Security Sprint	Can this issue area be addressed by planned revisions to Commerce's policy and guidance?
Risk assessment methodology	Commerce did not use a sound risk assessment methodology.	NIST did not use a sound risk assessment methodology.	Yes[a]
Documentation of key decisions	Commerce did not fully document facility security level (FSL) calculations NIST did not fully document decisions about countermeasures.	NIST did not fully document review of FSL determinations. NIST did not fully document decisions about countermeasures.	Yes

[12]OSY and NIST performed risk management steps for NIST's Gaithersburg and Boulder campuses in 2015, and NIST performed risk management steps for both campuses from February to May 2017, as part of its Security Sprint. We evaluated these activities against the version of the RMP Standard that was applicable at the time they were performed.

Issue area	2015 Risk management activities	2017 Security Sprint	Can this issue area be addressed by planned revisions to Commerce's policy and guidance?
Stakeholder involvement	Tenant agencies did not document agreement with Commerce's FSL determinations. NIST did not provide other tenant agencies with decision-making authority over recommended countermeasures for its campus in Boulder.	NIST did not provide other tenant agencies with decision-making authority over the FSL determination or recommended countermeasures for its campus in Boulder.	No[b]
Interagency Security Committee (ISC) Risk Management Training	Commerce assessors did not complete ISC training. NIST could not confirm that its decision maker completed ISC training.	NIST's assessors and decision maker did not complete ISC training.	No[c]

Source: GAO analysis of Commerce, NIST, and ISC data. | GAO-18-167T

[a]The draft policy requires assessors to use the ISC's Appendix A: *The Design-Basis Threat Report (FOUO)* when conducting assessments. As of 2016, Appendix A: *The Design-Basis Threat Report (FOUO)* identifies 33 undesirable events, but draft guidance accompanying the draft policy identifies 32 undesirable events. An undesirable event is an incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency. Office of Security (OSY) officials stated that the final policy will require assessors to consider all undesirable events identified by the ISC's standard on the risk management process.

[b]As of July 2017, Commerce's draft policy does not require agencies to establish a facility security committee at multitenant facilities or campuses.

[c]While the draft policy does not contain specific ISC training requirements, an OSY official said that assessors have begun to receive training and it is expected that all assessors will be trained by the end of fiscal year 2018.

Additionally, although OSY and NIST have taken some steps to align NIST's risk management process with the RMP Standard, the two entities did not coordinate their overlapping risk management activities. This could lead to duplicative efforts, hinder potential progress toward improving NIST's physical security program, and expose the campuses to risks.[13] Because NIST is currently developing its policy for performing its own risk assessments, it has the opportunity to incorporate a mechanism to ensure a high level of coordination with OSY, which could reduce overlapping activities, thereby minimizing the potential for unnecessary duplication.

[13]GAO-17-491SP. We have defined overlap as occurring when multiple agencies or programs have similar goals, engage in similar activities or strategies to achieve them, or target similar beneficiaries. We have defined duplication as occurring when multiple agencies or programs engage in the same activities or provide the same services to the same beneficiaries.

In our report released today, we recommend that the Director of OSY should ensure that the draft Commerce risk management policy is finalized and implemented in accordance with the ISC's RMP Standard, including requirements for risk assessment methodologies, documentation of key decisions, stakeholder involvement, and training. Additionally, we recommend that the NIST Director should finalize and implement risk management policies that ensure formal coordination between OSY and NIST and align with Commerce's revised risk management policy. Commerce agreed with our recommendations.

Chairman LaHood, Chairwoman Comstock, Ranking Members Beyer and Lipinski, and Members of the Subcommittees, this concludes my prepared remarks. I would be happy to answer any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

For further information regarding this testimony, please contact Seto J. Bagdoyan, (202) 512-6722 or bagdoyans@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions to this testimony are Gabrielle Fagan (Assistant Director); Amber D. Gray (Analyst in Charge); Georgette Hagans; and Elizabeth Kowalewski. Individuals who made key contributions to the report upon which this testimony is based include Elizabeth Dretsch, Justin Fisher, April H. Gamble, James Murphy, Carl Ramirez, and Shana Wallace.

Seto J. Bagdoyan
Executive Biography

Summary

Seto Bagdoyan is currently the director for audit services in GAO's Forensic Audits & Investigative Service (FAIS) mission team. During his GAO career, Mr. Bagdoyan has served in a variety of positions, including as legislative advisor in GAO's Office of Congressional Relations and as assistant director for homeland security and justice. He has also served on congressional details with the Senate Finance Committee and the House Committee on Homeland Security. In his private-sector career, Mr. Bagdoyan has held a number of senior positions in consultancies, most recently focusing on political risk and homeland security. He earned a BA degree in international relations/economics from Claremont McKenna College and an MBA in strategy from Pepperdine University.

Detail

Mr. Bagdoyan serves as the director for audit services in GAO's Forensic Audits and Investigative Service (FAIS) mission team. In FAIS, he has led a broad body of work related to fraud, waste, and abuse and the integrity of internal controls in various program areas including health care (Healthcare.gov enrollment), tax-debtors with security clearances, Hurricane Sandy disaster assistance, and concurrent military disability benefits.

Previously, Mr. Bagdoyan was a legislative advisor in GAO's Office of Congressional Relations where he covered the House Committee on Oversight and Government Reform and the Senate Committee on Homeland Security and Governmental Affairs. Mr. Bagdoyan began his GAO career in summer 1987 in the Los Angeles Regional Office before transferring to Washington, D.C. in summer 1994.

During his two tenures with GAO, Mr. Bagdoyan has also served as an assistant director in the Homeland Security and Justice team, where he led work on border and maritime security and critical infrastructure protection. Further, Mr. Bagdoyan has served on congressional details with the Senate Finance Committee and the House Homeland Security Committee where he led the planning and implementation of various oversight hearings and field investigations.

In addition to his GAO service, Mr. Bagdoyan has extensive experience in the private sector, having held senior positions in a number of consultancies focusing on risk management and homeland security. Mr. Bagdoyan has a B.A. degree in International Relations & Economics from Claremont McKenna College and an M.B.A. degree in Strategy from Pepperdine University's School of Business and Management.

Chairman LAHOOD. Thank you, Mr. Bagdoyan, and I want to thank all the witnesses for your valuable testimony here today.

The Chair recognizes myself for five minutes of questioning.

I guess I want to first start off and say that I've had the opportunity to watch the three videos a couple times now, and watching them and observing them, my reaction is disturbing, alarming, particularly when you think about the work that goes on at the NIST campus in Boulder and in Gaithersburg, the sensitive work, the strategic work, the proprietary nature of what goes on at these facilities, much of what relates to national security, and so when I think about what procedures are being put in place now, I'm anxious to hear today those, and Mr. Bagdoyan, I was going to start with you.

After learning of the incident involving the meth lab in 2015, you would think that there would be measures put in place that would prevent something like that or vulnerabilities from occurring. Today after hearing what steps have been implemented in your recommendations, what can you tell us to assure the public that these vulnerabilities have been taken care of? And then secondly, are you confident that if you were to do another undercover operation in the next month here, that those would fail?

Mr. BAGDOYAN. Mr. Chairman, thank you for your questions. I'll take the first one obviously first.

Based on what Dr. Rochford and Ms. Casias have mentioned, I think they are taking this seriously. That's good to know, and we look forward to receiving more details about what they plan on doing in response not only to our recommendations but also the incident you mentioned. There's going to be a long-term effort. I think what they both described are promising first steps. We are probably playing a long game here in terms of getting things done. So that would be for the first question.

The second question, it would definitely be speculative on my part to say whether or not anything that would be put in place would work, so I'll defer answering that one.

Chairman LAHOOD. And what about reassurances that you can give to the public that this has been remedied?

Mr. BAGDOYAN. Well, I can't say that it has been remedied. As I mentioned, these are first steps. They are promising. They are in the right direction. I'll hold the witnesses to their word that they are taking this seriously. They both outline various steps that they are taking. Management attention and priority is key, as Dr. Rochford mentioned. Training is an absolute must. To have a security culture, you have to train your people to take it seriously. So that would be my answer.

Chairman LAHOOD. Thank you.

Dr. Rochford, similar to you, give us your assessment on what reassurances you can give to the American people here today that you've taken these recommendations into account and that you're implementing them and that the vulnerabilities are no longer there.

Dr. ROCHFORD. I agree with the Committee that these breaches are unacceptable, and I do share your very, very deep concern. I also agree with my colleague from GAO. This is going to require a culture change. We have the responsibility—I have the responsi-

bility for keeping NIST staff safe and secure, and we have a responsibility, as you noted, to secure the substantial investment that the taxpayers have made to build NIST what it is today.

This breach, I agree, demonstrates the need for clear requirements, clear training, greater accountability, and we are undertaking all those steps.

Last month, I met with all senior leadership for a two hour security summit where we described the needs for accountability. Today, later today, I actually meet with all managers at NIST, and then we're going to have all-hands-staff security summits on both campuses that I will personally lead. We've developed training, and we'll have mandatory training, for all 3,500 and the several thousand associates. So I do agree, this is a bit of a long game. It's going to take time to have all this training done. But we will do it, and then I will personally ensure that the training is taken, and we will consider taking measures so we can understand the impact and the improvement in our security culture.

As mentioned, we did undertake a Security Sprint that has developed a number of prioritized activities, some of which I can mention here, some we can discuss in closed session, but we do have an action plan to address a number of issues at NIST.

Chairman LAHOOD. Can you talk a little bit about what you just mentioned there?

Dr. ROCHFORD. The Security Sprint?

Chairman LAHOOD. Yes.

Dr. ROCHFORD. What it did is, it certainly pointed out that we have a leadership issue. Culture is driven by leadership, and I need to take that responsibility to change the culture. So we are developing training. We have what we call baseline requirements, which will be our first training set. We then have additional training for things like criminal behavior, action plans, training for active shooter, other potential security issues. We have work where we're going to develop a Security Advisory Board. We're going to have an executive security committee so we can engage leadership on programmatic changes to ensure the culture sticks. We've taken some specific engineering and access controls that I can talk about in closed session, perhaps. We have a range of activities that we'll be undertaking over the year.

When the new confirmed NIST Director is on the job and starts, one of my first actions is my intent to brief him on these issues, show him the plans that we've undertaken, and with his permission continue these actions.

Chairman LAHOOD. Thank you, Dr. Rochford.

I now recognize Mr. Beyer for his questions.

Mr. BEYER. Thank you, Chairman LaHood, very much.

Mr. Bagdoyan, in the GAO report you write about the fragmented approach to security, which as a person interested in management and leadership for a long time, seems pretty nonsensical, too many cooks in the kitchen. You've got big Commerce responsible for the outside piece, NIST responsible for the cameras and the locks, and how did this divided approach come about and what can we do to fix it?

Mr. BAGDOYAN. Thank you for your question, Mr. Beyer. I think in the first part, it originated back in late 2015, I believe, once

NIST received, or Commerce received delegated authority for NIST police to act as federal law enforcement agents. So that was delegated by the Federal Protective Service. And then in 2017, the American Innovation and Competitiveness Act essentially directed Commerce to have an overall role in setting security policy and practice but also NIST maintained its ability to perform its security-related duties as it saw fit consistent with its culture that it was trying to build at that time. So in a very high level, that's the origin of the split.

I would agree with you that having a split situation like this is not really consistent with best practice according to federal standards, and it does lead to inefficiencies, especially when the two parties really don't coordinate or collaborate. Sometimes it's fine to have two distinct streams of oversight over a major program like this, but if they don't talk with each other, they end up doing separate risk assessments and so forth. That is definitively counterproductive and hinders effectiveness overall.

Mr. BEYER. In your perception, we'd probably need to amend that Act in order to be able to centralize the security?

Mr. BAGDOYAN. Well, that certainly would be one option. That would be up to Congress. It's certainly not for me to prescribe but I think in the past it has been noted that in order to fix this, I believe one of the assessments that NIST did pointed out that the only remedy was a statutory fix. On the other hand, we know of no plans to pursue such a fix at the Department level.

Mr. BEYER. Very good. Thanks.

Dr. Rochford, I was in an embassy overseas for four years, and every night the Marines would go office to office and look at the stuff on everyone's desk, and if somebody had classified material out, there was a report the next morning, and the very—and no one wanted to have a report which came back to Washington. Is there any reporting program like that at Boulder or in Gaithersburg, where it's a guard who lets somebody in who shouldn't have been let in with a bad badge or papers left out on desks that shouldn't have been let out?

Dr. ROCHFORD. We do have incident reporting on both campuses that then bubble up through our police staff, which are managed by OSY to the Director's office. For example, I know that in Boulder, the doors are checked nightly and they provide a report of any issues that then can be addressed either through maintenance or through personnel action.

Mr. BEYER. When you mentioned that you built security into the employee performance plans——

Dr. ROCHFORD. Yes.

Mr. BEYER. —is this tied to incident reporting then?

Dr. ROCHFORD. Right now it addresses the baseline security requirements. The baseline security requirements do address reporting incidents of tailgating, piggybacking, things of that nature.

Mr. BEYER. Have you figured out a way to keep paragliders from landing on your campuses?

Dr. ROCHFORD. That might have some technology solutions that we've not addressed.

Mr. BEYER. And Ms. Casias, in your oversight role, do you envision a way for you at OSY to be able to provide the necessary over-

sight of the security that NIST provides without necessarily having to own half of it directly?

Ms. CASIAS. Congressman, we recognize, and Dr. Rochford and I have talked about this, we recognize that the security management structure does require some evaluation, and we agree with GAO. We've accepted their recommendation. So I think we do have work in that area. We've already started some steps. We've identified executive sponsors, myself and Dell Brocket, the Associate Director for Management Resources at NIST. We'll lead that endeavor. We've selected internal teams. We're also looking at using outside security experts such as folks from the ISC to help us in that matter. In our review, we'll be looking at roles, responsibility and accountability and how that impacts security.

So I think there's a mix. There's not one-size-fits-all, and we know that the Boulder campus is different from the Gaithersburg campus, so we will be working jointly but we do agree that this is an item that we do need to look at and is a serious item that needs attention immediately.

Mr. BEYER. Thank you, Mr. Chairman.

Chairman LAHOOD. Thank you, Mr. Beyer.

I now recognize the Chairman of the full Committee, Mr. Smith, for his questions.

Chairman SMITH. Thank you, Mr. Chairman.

Mr. Bagdoyan, let me address my first question to you, and that is, how much confidence do you have that the GAO's recommendations will be implemented by NIST?

Mr. BAGDOYAN. Good question. I really believe this. I am confident that based on what I've heard this morning certainly in its official response to our draft report that Commerce and NIST are taking this seriously and they'll take the necessary action.

Chairman SMITH. I mentioned in my opening statement that unauthorized access was attempted by the GAO at both campuses 15 times, and 15 times they were successful. It just seems incredible that that would be the case, but to what do you attribute that other than just lax security? And is there any excuse for that? I don't know where to——

Mr. BAGDOYAN. I take your point, Mr. Chairman. I'll probably be best served to respond to that in a closed session.

Chairman SMITH. And as I understand it, it's the Department of Commerce that came up with the designation "law enforcement sensitive." Is that right?

Mr. BAGDOYAN. That's correct. They are the marking agency in this case.

Chairman SMITH. Ms. Casias, I'd like to ask you about that designation, "law enforcement sensitive." Why did you choose to apply that to the three videos that members saw in closed session before we opened it up for this hearing?

Ms. CASIAS. We believe in viewing the videos, which I have viewed and so has Dr. Rochford, that there are security vulnerabilities that other folks could look at and use those vulnerabilities within our facilities or other federal facilities. In addition, I'd be more than happy in any closed session that we could get into that in a little more detail so——

Chairman SMITH. What is the definition of "law enforcement sensitive"?

Ms. CASIAS. The definition is that it's the sensitivity if that came out would cause some issues with security within our campuses.

Chairman SMITH. Okay. Can you give me—do you happen to have the exact definition with you?

Ms. CASIAS. I do not have that with me but I can get that for you.

Chairman SMITH. If you can get that fairly quickly, that would be helpful.

My suspicion is that you all maybe overly cautious. Having seen the videos, they're pretty obvious as to what might cause breaches and what did cause breaches in this case, and I don't think it's revealing much to acknowledge that. In fact, it may even be helpful. So I'd like to see the exact definition and see what the rationale was for applying it in these cases.

Ms. CASIAS. Absolutely.

Chairman SMITH. And I might even ask you to go back and take another look because while you want to err on the side of caution, you also don't want to prevent information that can and should be seen by others from being considered by others as well.

Let me go to Director Rochford and ask you a couple questions to the extent that you can answer them, and that is, just generally what can be done to prevent some of these unauthorized accesses? I know you responded to the Chairman generally. If you want to elaborate on that, I think that would be helpful.

Dr. ROCHFORD. So if we're talking about the specifics in the video, I mean, generally, we see security as a layered approach so we need to have both improved training and improvement in our security force that does their checks, but the other layer is the employees, and part of what I need to do is make sure that NIST staff have a much greater awareness about these concerns, know at some level how these things can be spoofed, for example, and through training and I think this awareness, we can have them also do a better job of making the appropriate checks to ensure security and avoid breaches.

Chairman SMITH. And I assume improvements have been made to security in the last several weeks?

Dr. ROCHFORD. When I started, the security plan actually became operational over the last couple months so we have developed training materials. We have video training materials. We have a number of things that I'll be launching very soon. So yes, we're ready to——

Chairman SMITH. Would the security measures that have been implemented recently have prevented the unauthorized access that has occurred in the past?

Dr. ROCHFORD. I think the training is going to be a key part of that, and the training is going to take some time. So we have not put in place something that would cause 100 percent improvement.

Chairman SMITH. What has been put in place that you guess would prevent most of the unauthorized access from occurring?

Dr. ROCHFORD. There are some items that I could discuss in closed session.

Chairman SMITH. I'm not asking you what those items are. I'm just asking you generally to say whether or not you feel that what's already been implemented would prevent most of the unauthorized access that has occurred in the past.

Dr. ROCHFORD. I think we've put things in place to improve the situation.

Chairman SMITH. Okay.

Dr. ROCHFORD. I do not have confidence that I could say we have 100 percent——

Chairman SMITH. Thank you very much.

Thank you, Mr. Chairman.

Chairman LAHOOD. Thank you, Chairman Smith.

I now recognize the Ranking Member, Mr. Lipinski.

Mr. LIPINSKI. Thank you.

Ms. Casias, your office overseas the Commerce Office of Security, which manages the Police Services Group. The Director of Security for NIST provided a letter to the Science Committee on September 14 of this year that the Police Services Group in both Colorado and Maryland had a total of 41 authorized staff with five current vacancies under the existing operating budget. Can you tell us what sort of impact you believe current budget constraints have on NIST's security posture, and what can we in Congress do to help in that regard?

Ms. CASIAS. Congressman, thank you for that question. As we said, security is not one-size-fits-all, and while we have our police force, our Police Services Group, we also have contracted staff which we have supplemented that workforce with. At this point I believe looking at our risks and our vulnerabilities, we are working within our budget and believe that we have adequate funding. As we work through the evaluation and look at the different responsibilities between NIST and the Department, if there is anything there we'll identify and work with this Committee on those findings.

Mr. LIPINSKI. Let me ask Dr. Rochford or Mr. Bagdoyan, do you agree with that in terms of having enough resources?

Dr. ROCHFORD. At this point we've gone through our Security Sprint and have identified a number of activities that we can make. I currently believe I have the resources to take on that first tranche of activities. So at this time I believe we have the resources.

Mr. LIPINSKI. Mr. Bagdoyan, do you have any thoughts on that?

Mr. BAGDOYAN. Yes. Thank you, Mr. Lipinski. I would answer in terms of the resourcing level as a function of the risk and the countermeasures already in place and anticipated, so a precise number that would drive a budget is obviously a function of that, and I would defer to the Department on that matter.

Mr. LIPINSKI. Thank you. Mr. Bagdoyan, part of the GAO examination of NIST security included a survey of NIST employees which you had talked about in your testimony. My understanding is that the sample for that survey was exclusively technical and scientific staff. Is that true, and if so, why were other staff omitted from the survey pool?

Mr. BAGDOYAN. Yes, that is correct, Mr. Lipinski. We surveyed approximately 500, which is a projectable sample, and a determina-

tion of what to include and what not to include was essentially a methodological one. We can provide you with additional detail separately if you like in terms of how we arrived at that.

Mr. LIPINSKI. Was there a reason that the administrative staffers were not included in that?

Mr. BAGDOYAN. Well, I don't recall the specifics but I would say that we chose to focus on people who would likely encounter potential intruders and others during the course of their duties.

Mr. LIPINSKI. But it would seem like anyone coming in to the gate would be someone who potentially would have the possibility of letting someone in who shouldn't be in there.

Mr. BAGDOYAN. Yeah, I take your point but we just chose what we chose, and I can certainly provide a more detailed explanation on the methodology separately.

Mr. LIPINSKI. Okay. You said 75 percent in the survey said that they take security—I forget, what were the exact——

Mr. BAGDOYAN. Yes. Let me look at my cheat sheet here. It says about three-quarters of scientific and technical employees believe that NIST leadership places great or very great importance on physical security issues.

Mr. LIPINSKI. Is that 75 percent enough?

Mr. BAGDOYAN. Well, optimally you would want it to be 100 percent. That was—that goes back to my earlier point that if you want the culture to improve, the awareness to improve, and be optimal, you really need to be at a very, very high level for this to work. Otherwise a single weak point, a single individual who might not get it is a potential vulnerability.

Mr. LIPINSKI. It sounds like there's good work being done. We certainly need to follow up, and the culture I think is certainly going to be a big issue.

Just very briefly, do you think there's any—is it possible that the type of people who would be working, the technical people who would be working at NIST are people who are used to more open circumstances, campuses, things like that that do not require the type of security and that could be a reason why?

Mr. BAGDOYAN. It's certainly a possibility but again, with proper training, leadership emphasis, you move the needle in the direction it needs to go, and awareness is key. Prioritization from leadership is key as is getting stakeholders, for example, on the Boulder campus. There are other agencies that share the space to get them involved as well because their culture would be also impacted, and that's a key point.

Mr. LIPINSKI. Thank you.

I yield back.

Chairman LAHOOD. Thank you, Mr. Lipinski.

I now recognize Mr. Marshall of Kansas for his questions.

Mr. MARSHALL. Thank you, Chairman LaHood.

First question for Mr. Rochford. In the military or in business when we have a big goal, a big vision, we typically set out a timeline with major events, major milestones, so our goal here obviously I would assume we have all the same goal: better security in these facilities. Do you have a timeline? Where are we on that timeline? Where's it going?

Dr. ROCHFORD. Our Security Sprint did set out a timeline for phase I for this training, this outreach, the accountabilities. That timeline has various things happening that I've mentioned with our goal to have complete mandatory training, for example, by the end of the calendar year.

Mr. MARSHALL. Can we have access to that, perhaps? Would that be a reasonable question?

Dr. ROCHFORD. That's to the——

Mr. MARSHALL. To the timeline or——

Dr. ROCHFORD. Certainly. I don't have it with me but I can provide that.

Mr. MARSHALL. Okay. Thanks.

I want to go back to the plutonium incident at the NIST facility in Boulder, Colorado. I guess that's several years ago. Obviously it created some significant challenges to not just the facility but the surrounding people as well. And now we're aware of another incident at the same facility. Do you feel like you've done everything possible to shore up that situation there for such another dangerous event? Obviously there's some pretty toxic things going on there.

Dr. ROCHFORD. Plutonium was a wake-up call for NIST. That was the moment we realized that our safety culture was not what it needed to be. In the past we've worked on what is considered an expert culture where we trusted our highly trained individuals to take on safety. What we recognized is, we needed to take this more deeply. We needed to have specific training, specific processes, specific access controls and procedures. As a result, I could state that we have a very assertive safety culture now, and in fact, that's what I'm modeling our changes in the security culture towards. In fact, that specific event we basically met all the Nuclear Regulatory Commission's requirements satisfactorily. We've made great strides in our safety program both in radiation—radioactive materials and safety in general, and I think yes, our safety program is much more robust.

Mr. MARSHALL. I'm just curious. The people that are doing the research are scientists. Are they the ones ultimately in charge of the security, figuring out what—I mean, I'm guessing it's two different people. My doctors are not real—the surgeons are not real good at figuring out what to do in the ER. So I'm hoping it's different people than the scientists trying to figure out a security program for the facility.

Dr. ROCHFORD. No. So the way we operate is, we obviously have a management structure. I as the Acting Director have responsibility for security. We can gather scientific input. So for example, when we assess a space, as the Chairman had mentioned, we may have proprietary information, we may have other information. We gathered that from the scientists so we can understand what sort of safety and/or security protocols to put in place. Those then are developed in programs that follow guidelines created by both the Department's Office of Security and then the local controls that we have in place.

Mr. MARSHALL. Okay. My last question. Going back to Boulder, there's still no external barrier in Boulder as I understand it. Do you feel like that's a problem, and what are we—why isn't—I

mean, that would seem to me to be more of an immediate solution to unauthorized access to restricted areas or some type of a physical external barrier. Do you think it's necessary? Why haven't we done it, or is that a waste of time and effort and money?

Dr. ROCHFORD. I would not characterize it as a waste of time and effort. When I started in January and undertook the Security Sprint, my goal was to be able to get quick wins, to be able to do things that we could take action on quickly. A fence in Boulder, it's going to be a multi-stakeholder process. There's a number of factors and considerations including both the city, the neighbors, local government, issues of that nature. There are environmental aspects. It's something that will take a longer time.

Mr. MARSHALL. That just drives me crazy to think about that, that here's an immediate danger and we're not—and the process, the rules, the regulations, and again, having built a hospital facility, I know what it's like. It just takes months and years to go through the process, and in the meanwhile, we can't get to the real solution.

So I look forward to going through those weeds as quick as you can and making these places secure.

Thank you, and I yield back.

Chairman LAHOOD. Thank you, Mr. Marshall.

I now yield to the Ranking Member, Ms. Johnson, for her questions.

Ms. JOHNSON. Thank you very much, Mr. Chairman.

It's rather puzzling to me when you put everything on training, what was the initial training when people were hired? Do you have any standards, ethical standards for them to have a commitment? Yes?

Dr. ROCHFORD. We do have onboarding training. In retrospect, onboarding training has been rather simplistic—wear your badge. What I need to do is develop—and we have done this—a training that's very explicit, very unambiguous, and actually includes various scenarios so people know precisely what we mean and what we expect. So I think in the past we just had not done training that was sufficiently detailed, and that is being remedied.

Ms. JOHNSON. You know, I'm having a hard time. I fully support the work of NIST, and I looked at the recommendations that GAO has recommended, and I'm having a very hard time understanding what changes were made or what kind of approaches did you make after these incidences. It seems very, very loose to me in a very important area. Do you feel capable of running this agency and keeping the activities at a professional level?

Dr. ROCHFORD. Yes, I do. I've been in this role since January so I've had a limited span here that I can do these things. Since 2015, we have added several engineering access controls. We did increase security staffing. We did establish this NIST Security Advisory Board. But there is more to do, and that's what I've been working on over the last many months, and I'm confident when our new Director joins us that he'll be interested in moving this forward as well.

Ms. JOHNSON. When you say there's much more to do, give me an idea what else that you have in mind to do.

Dr. ROCHFORD. In addition to training—this is a culture change, in my opinion, so it requires a leadership commitment that's consistent and persistent, right? We need to continually meet with staff. We need to demand that the training requirements are met. I need to hold my management accountable. My management needs to hold the employees accountable. We basically have to change an attitude so that we're doing this in the best possible way. We've done it in safety. We know how to do this, but we also know it takes time and it takes real commitment. So I have the commitment. We just need some time.

Ms. JOHNSON. Okay. Ms. Casias, do you have any comments?

Ms. CASIAS. Yes. I agree with Dr. Rochford that it is a culture change, but I also believe as we're working together we need to look at the management structure. That is a priority for us. We also—as I stated, we now have all of our staff trained on the ISCR RMP standards, and I think looking and working with those facility assessments and getting those relooked at this year, redone, and looking at that jointly, I think it really is critical that we have that open communication and working together, and I believe we do. We've talked about a lot of trainings today, and those are not just the NIST folks working on that. Our Director of Security, who is on campus at NIST, has been working, and yesterday just had one of the security days with a fabulous turnout from the staff, and that was a joint effort and working together and looking at what we need to do.

So there's more to do than training, and I believe we're on that path and we're working towards that, and I'm confident that our partnership together we will get there.

Ms. JOHNSON. Have you looked at these? Are you following the recommendations of GAO?

Ms. CASIAS. Absolutely. We have already started. As I noted, we've already put together—both myself and Dell Brocket, who's in the room, we're going to be spearheading this and the executive sponsors. We've actually worked on other projects in the Department before this, and we've been successful, and I know that we'll be successful in this one, and it's a priority. Security is a priority for the Department, for our people, for our assets and our information.

Ms. JOHNSON. Well, thank you. I know that security is very important but I'm talking about the ethical behavior of the people within a security measure as well.

Ms. CASIAS. I agree, and I think looking—and there's been some steps of initiating some security measures in people's performance plans, but we are looking into the incidents that, you know, folks have seen on the videos and determining—we've done appropriate counseling to date and we're working with the appropriate offices on what other steps we need to take.

Ms. JOHNSON. Thank you very much.

Chairman LAHOOD. Thank you, Ms. Johnson.

I now recognize Mr. Norman from South Carolina.

Mr. NORMAN. Thank you.

Dr. Rochford, I guess as a follow-up to Chairman Smith's question about the 15 attempts and you had 15 breaches, and you mentioned that if they occur today, you couldn't give 100 percent guar-

antee that be—it would prevent it. What percentage would you give?

Dr. ROCHFORD. That would be difficult to assess. At this point because we haven't rolled out the training, I don't think some of the early steps that need to be taken have occurred. The training, I will have the meetings with management this afternoon, and again, these have been planned for some time. I'll have meetings with all staff. At that point we'll roll out the required training. My belief is as people take the training and we're holding them accountable, we'll see improvements.

Mr. NORMAN. Okay. Now, I also understand that the Gaithersburg, Maryland, campus has a nuclear reactor on site. Is that true?

Dr. ROCHFORD. That's correct.

Mr. NORMAN. NIST stores caches of radioactive material for testing. Is that true?

Dr. ROCHFORD. Testing and standards, measurement standards, correct.

Mr. NORMAN. Do you realize you can google this and get this on site? You don't see this as a security risk?

Dr. ROCHFORD. Some of this will be known because of Nuclear Regulatory Commission postings so, yes, it is known. In addition, our nuclear reactor is a center for neutron research, which is a center that uses neutrons to do measurements and therefore we interact with industry and academia so they do know about it as well.

Mr. NORMAN. And another question, Doctor. According to the Washington Post, in August of this year a NIST employee was exposed to unsafe dose of radiation, and according to this article, as of September 27, it's still unknown how the container of the radioactive material was compromised. Have they found anything out on that?

Dr. ROCHFORD. Yes, yes. We've learned a great deal in that incident. The material is known as americium. It was held in a small 50-milliliter ampoule. We received it from an energy lab about 17 years ago. It was in solution, and as the radioactivity occurred, these decayed particles caused what they call radiolysis, created a gas, and over time the gas overpressured and the ampoule exploded. So what in fact happened was not a mishandling event but we keep these in these lead storage containers, and the material burst. We found it during a routine radiation testing, a survey program that we have where we look at these spaces weekly, and then when we found it, we could put controls in place, and then we had to test all the individuals who had been in contact with the material before the breach or before the dispersion was noted.

We're very aggressive in our reporting in safety, so we immediately went to the Nuclear Regulatory Commission, and we provided a notification that had worst-case scenarios. What we've learned since as we've been able to do more testing both of the material and the bioassay, we believe that the individuals involved have not had exposures above the regulatory limits, that they've actually been below the regulatory limits. These measurements are actually quite difficult. These are alpha emitters, which are very, very faint. It also took some time for us to get the measurements. But we have engaged with the Nuclear Regulatory Commission at great length and with the Department of Energy, and in fact, the

30-day report to the NRC went out Saturday, so that's a public document.

Mr. NORMAN. Okay. You know, I join in Congressman Johnson I guess and the concern I have is that you all were taking it seriously and particularly with the taxpayer dollars that are going toward this that it's—I see it's a leadership problem but still there's got to be some consequences to it, so I would ask you to put this at the top of your list to get fixed, and not just addressed but to get fixed because 15 of 15 breaches is not—is unacceptable in my mind.

Dr. ROCHFORD. I agree.

I yield.

Chairman LAHOOD. Thank you.

I now recognize Ms. Bonamici of Oregon, please.

Ms. BONAMICI. Thank you very much, Mr. Chairman.

Dr. Rochford and Ms. Casias, NIST now has, it's my understanding, your full-time equivalent police officers, about 28 in Maryland and 13 in Colorado, but you also use contract protective security officers. So can you talk a little bit about what they do, where are they stationed, at the gates, at the doors, and what training do they get and what is the turnover among those contracted protective security officers?

Ms. CASIAS. Thank you for your question. I will have to get back to you on the turnover. I don't have that information with me immediately. But all of our contractors are required to have certain standards. We do provide training, and I can tell the folks on this panel that we have provided training since the penetration issues that we've had, and we'll continue to have that training with those folks.

Ms. BONAMICI. How does their training compare to the, for example, police officer training?

Ms. CASIAS. I would have to get back to you on the exact distinctions between the both, but in the case of providing the security services, both parties, the Police Services Group and the officers, the contract force, receive the same training, and everyone that is responsible for that understands that it is totally unacceptable with the breaches and what has happened.

Ms. BONAMICI. Thank you. I would appreciate the follow-up on the turnover among those contracted officers.

The 2015 incident, which we've all heard about with the NIST employee who was a NIST police officer trying to make meth, now that of course is a rare type of situation but what recommendations are you making now that would have prevented that particular incident as opposed to your recommendations to keep out unauthorized access? This person was a NIST employee, so what specific recommendations would have prevented that? Ms. Casias or Dr. Rochford?

Ms. CASIAS. I obviously was not in my position when that occurred but I know we have put more—instituted more, looked at how we're using rovers, how we're using our police force and our guards and our actual police force that's on site.

Ms. BONAMICI. But he was a police officer, so what——

Ms. CASIAS. I agree.

Ms. BONAMICI. What would have prevented that at the time? What are you doing now that would have prevented that?

Ms. CASIAS. I believe how we are running our shifts and looking at our shifts, that may have prevented it. I'll have to get back to you, you know, on exact measures that we may have taken.

Ms. BONAMICI. Thank you.

Mr. Bagdoyan, the GAO report notes inefficiencies, plural, that arise from the fragmented organizational structure of NIST security. An example mentioned in the report was that NIST is responsible for procuring and placing the security cameras but the Department of Commerce is overseeing the police personnel and the facilities, and that led to some of the security cameras being placed in locations that weren't particularly useful or helpful for the police. So what are—number one, what are some of the other inefficiencies, because you said inefficiencies, and that was one example? And then also, how could that have been prevented. It seems like maybe a simple phone call could have said—could have remedied by saying, you know, the cameras aren't in the right place. So how did that happen? And maybe I can get Ms. Casias and Dr. Rochford to respond as well.

Mr. BAGDOYAN. Sure. I'll let my fellow panelists here respond from their perspectives.

In terms of placement of equipment and so forth, I certainly wouldn't venture there in an open hearing, but in terms of other inefficiencies, you have risk assessments that are done separately, for example, so that is a core function that at least should be coordinated, if not collaborated on.

Ms. BONAMICI. And I see Dr. Rochford nodding his head so I'm assuming that NIST agrees with that.

Mr. BAGDOYAN. Right. So that's—right. So I would just leave it at that. That's a key inefficiency.

Ms. BONAMICI. Thank you.

Mr. BAGDOYAN. And also crafting different policies at times. Parallel security policy is another area of inefficiency that at a minimum should be much more closely coordinated if——

Ms. BONAMICI. Thank you, and I don't want to interrupt but I want Dr. Rochford and Ms. Casias to respond to the, how could that have been remedied? Is there some channel for—a better channel for communication where if the cameras are put in the wrong place, why weren't they—why wasn't that immediately fixed?

Dr. ROCHFORD. That should have been immediately fixed. I don't know what line of communication dropped and why that didn't occur. On our campuses, our cameras and other access controls are not used purely for security as well. We do have some that are put in for safety reasons, and it could be that security personnel were concerned that they may not have had appropriate access but those were done for programmatic reasons.

As far as coordination, our Security Advisory Board does have our local OSY Director of Security at NIST on that board, so when we do develop local policies, this individual is involved and weighs in. So we have worked to coordinate to ensure that we have the right amount of overlap.

Ms. BONAMICI. Thank you, and I see my time is expired. I yield back. Thank you, Mr. Chairman.

Chairman LAHOOD. Thank you. I now yield to Mr. Loudermilk of Georgia for his questions.

Mr. LOUDERMILK. Thank you, Mr. Chairman, and I thank the panelists for all being here today.

As has been mentioned I'm sure many times in the last few months and even here today, the incident with the police officer who was cooking meth in one of the laboratories, it's interesting, it was last year or in the last Congress I was Chair of the Oversight Subcommittee, and we were investigating this instance, and it was during that investigation when we actually uncovered the plutonium incident. In fact, it was an email. The question was, why wasn't Congress notified of the meth explosion, and an email we uncovered between two senior-level people was well, we didn't notify Congress about the plutonium incident either, and it was a thousand times worse. So I'm just bringing that up to say I hope that the communications with Congress would—is going to drastically improve with instances.

But I want to direct my questions to our response, Congress's response, regarding security issues that have transpired at NIST. Last year I sponsored the NIST Campus Security Act, which ultimately was incorporated into the American Innovation Competitiveness Act, which was signed into law back in January. Now, according to GAO report, physical security at NIST was split between the Office of Security and NIST, and the American Innovative Competitiveness Act directs the Secretary of Commerce to oversee law enforcement at NIST by establishing the NIST Director of Security. I understand that has been fulfilled, that position. How—are we seeing that with this new position, the new Director is closing the gaps that existed in security between the two offices, Dr. Rochford?

Dr. ROCHFORD. Yes, I would agree, and I think one activity is the Security Advisory Board in which he works. We also have weekly meetings between the Office of Security, Director of Security of NIST and our Emergency Services Office Director every week so we can make sure that day-to-day issues are dealt with.

I would like to note in terms of the plutonium incident, I wasn't in this job.

Mr. LOUDERMILK. Yes, I understand.

Dr. ROCHFORD. However, NIST would never keep things from the Oversight Committee, and that incident in fact did have extensive hearings at the time, so we were very forthcoming and did inform Congress during that incident as well.

Mr. LOUDERMILK. Mr. Bagdoyan, I know that the bill that I was referencing assigns GAO to conduct a study evaluating the performance of NIST Police Service Groups. Have you been able to assess the improvements or the performance that we've seen out of security since the new Director has been put into place?

Mr. BAGDOYAN. Well, not really. I mean, basically what our work consisted of was testing what was in place at the time. Obviously having a Director in place is important but what we're testing is the reality on the ground so the Director has to make things happen on the ground for us to be able to go back at some point, Con-

gressional direction, of course, to take another look and see how things have changed.

Mr. LOUDERMILK. Now, of course we don't want to get into areas that are sensitive to reveal——

Mr. BAGDOYAN. Of course.

Mr. LOUDERMILK. —anything in this session but I don't know the exact time frame of the videos that we saw earlier.

Mr. BAGDOYAN. Sure.

Mr. LOUDERMILK. But if those occurred within the past year, I still have concerns that we have not made strides in the right direction.

Mr. BAGDOYAN. Right.

Mr. LOUDERMILK. Is there still a lot of improvement that needs to be done?

Mr. BAGDOYAN. Yes, we can certainly try and address that point, Mr. Loudermilk, in a closed session.

Mr. LOUDERMILK. Okay. Thank you.

Dr. Rochford, do you agree that we still have a lot of area that needs to be covered?

Dr. ROCHFORD. Absolutely.

Mr. LOUDERMILK. Okay.

Dr. ROCHFORD. And as I'd mentioned, a lot of this is driven by culture, and that we can change.

Mr. LOUDERMILK. Thank you.

Since I have a few more seconds, Mr. Bagdoyan, in your testimony you described overlapping risk management activities. To what extent did you witness duplicative activities and what are the consequences of such duplication?

Mr. BAGDOYAN. Well, witnessing obviously is performing the assessments themselves, then devising security policies that are at least in part derived from those assessments. If they're not sufficiently coordinated and essentially collaborated on, then you might end up having two different lines of thinking in terms of what is risky and what the countermeasures are and what resources are needed to be devoted to those countermeasures.

Mr. LOUDERMILK. Thank you. And Dr. Rochford, this—you're inheriting a lot of the problems that existed, and just my final question, do you have a plan in place to reduce the duplication between the two?

Dr. ROCHFORD. Yes. In fact, much of what I think was seen as duplication was in fact coordination. We've often started our work using from documents derived from the Office of Security. As a manager I do have to make some resource allocation decisions so clearly those are things I can do in conjunction with the Office of Security. But we do that through coordination with our Security Advisory Board, which does have OSY and its personnel.

Mr. LOUDERMILK. Thank you. I yield back.

Chairman LAHOOD. Thank you.

At this time we recognize Mr. Perlmutter for his questions.

Mr. PERLMUTTER. Thank you, Mr. Chair.

Mr. Bagdoyan, how often does the GAO conduct kind of investigations like this where you do, I mean kind of sting operations, if you will? I'm familiar with TSA operations where sometimes you

go in and see if you can sneak through the security there. How often do you guys do this?

Mr. BAGDOYAN. Well, they do take a lot of time to develop and implement. Of course, all of our investigative work is derived from Congressional requests so we do get them periodically. You're absolutely right about TSA and the transport sector overall. We have done, as you may know, in the past work looking at the Affordable Care Act and its enrollment controls. I testified on that on several occasions in recent years. We most recently completed work on the FCC's lifeline program where we used undercover resources to attempt to enroll into the program, and we were mostly successful. So it basically runs the gamut. Again, it's driven by Congressional interest and request so we play in various different spaces, and I would point out that no one investigation is the same as another. They're all very unique.

Mr. PERLMUTTER. Thank you.

So Dr. Marshall is from Kansas, and he has questions, Dr. Rochford, about the Boulder campus and putting up a fence. So just listening to this, I think you've got to bifurcate between safety and security. They're two different things. So the plutonium was a safety issue. It wasn't like somebody was stealing it. But the security issue is, you have a guy roaming around the campus through an open window, for goodness sakes, for hours before anybody discovered him. So I don't know about putting a fence up in Boulder. That's going to take forever to get something like that done, but you certainly can harden the security for each building. What steps are you taking on that?

Dr. ROCHFORD. That's absolutely correct, and we have taken a number of steps in that regard. We've added additional engineering controls at the perimeters of the buildings. We've improved internal alarming in areas where we have windows of that nature. In fact, it wasn't an open window. What it was, was a temporary window in which we were doing laser experiments on the mesa, so it was easily broken. Now that's——

Mr. PERLMUTTER. That's been fixed?

Dr. ROCHFORD. There's other things we can—yes, that's been fixed, and we can talk about details.

Mr. PERLMUTTER. All right. Let's talk about the plutonium for just a second, and obviously in our area, we've dealt with issues pertaining to plutonium with Rocky Flats and all of that. I guess just as a neighbor of this laboratory, I wasn't aware that you guys were a storage facility. You're a laboratory. And to the degree that you are a storage facility, I hope that that's part of the approach you're taking, and I'd say to Commerce as well, that should be going to the Department of Energy or somebody else. You can react to that if you will.

Dr. ROCHFORD. So in fact, we are not a storage facility. In that particular incident, we had an exceedingly small quantity of plutonium that was being used to measure sensors and detectors that were going to be used for non-proliferation activities. However, there is no exceedingly small amount of plutonium, so we had to manage it very carefully. Since then we have only in Boulder used what are known as sealed sources.

Now, in Gaithersburg, we have a radiation physics division. We do have a number of sources, and these are used as measurement standards to calibrate things as diverse as radionuclides for medicine to things for non-proliferation for other activities.

Mr. PERLMUTTER. So I just—now I'm going to get on my political high horse for a second. I mean, obviously I'm listening to my friends on the Republican side of the aisle talk about radiation and these small amounts and the danger that comes from it, and I would just say as I just did in the Financial Services Committee, the President just openly talking about nuclear arms and building of stockpiles and all of that stuff, there's real danger there, and we all know that, and that rhetoric is dangerous, and so with that I yield back to the Chairman.

Chairman LAHOOD. Thank you, Mr. Perlmutter.

I now recognize Mr. Higgins of Louisiana for his questions.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Bagdoyan, as Director for the GAO's Forensic Audits and Investigative Services, I thank you for your service to your country, sir.

Mr. BAGDOYAN. Thank you.

Mr. HIGGINS. Looking at your bio, you have an extensive background of security, critical infrastructure protection, risk management, and homeland security. Would you concur that you're an accomplished investigator?

Mr. BAGDOYAN. I would like to think so.

Mr. HIGGINS. One would like to think so. My background is in law enforcement, sir. Would you also agree that it's just human nature that over time if there's been no critical incident, there develops sort of a relaxed culture of security at entry and perimeter security? Would you concur that that's generally true and——

Mr. BAGDOYAN. Yes, it's possible that over time that happens——

Mr. HIGGINS. Thank you.

Mr. BAGDOYAN. —if you don't pay attention.

Mr. HIGGINS. However, given the incidents of July of 2015 and April of 2016, those security breaches, wouldn't as an experienced and accomplished law enforcement professional and security expert, wouldn't you concur that the heightened awareness should have existed by the time your agents began your undercover probes?

Mr. BAGDOYAN. That would be a logical response, yes.

Mr. HIGGINS. And it was your team that conducted the security evaluation of NIST. Is that not—is that correct?

Mr. BAGDOYAN. Yes. My investigative colleagues performed that work.

Mr. HIGGINS. How many individuals made up the team of GAO undercover staff?

Mr. BAGDOYAN. That I will defer answering until a closed session.

Mr. HIGGINS. I understand. Was there more than one agent?

Mr. BAGDOYAN. I'll reserve on that one. Thanks.

Mr. HIGGINS. Your one or potentially more than one were quite successful though, were they not?

Mr. BAGDOYAN. That's what the record shows, yes.

Mr. HIGGINS. At any point during the course of your undercover investigation did the GAO agents have potential access or were they in a close vicinity of a NIST computer?

Mr. BAGDOYAN. I'll have to defer answering that, sir, sorry.

Mr. HIGGINS. Were they in a building where computers existed?

Mr. BAGDOYAN. Same answer.

Mr. HIGGINS. Would your staff have had the opportunity to insert a thumb drive on one of these perhaps nonexistent computers——

Mr. BAGDOYAN. I'll——

Mr. HIGGINS. —thereby infecting the system with a virus?

Mr. BAGDOYAN. I'll defer answering that.

Mr. HIGGINS. Did your staff have access to laboratories?

Mr. BAGDOYAN. Same answer.

Mr. HIGGINS. So in these buildings that your staff was able to enter, is it reasonable to presume that there were offices with computers and perhaps laboratories, given the fact that that's why these buildings exist?

Mr. BAGDOYAN. That's what NIST exists for so that's a safe assumption.

Mr. HIGGINS. It would be a reasonable presumption, would it not?

Mr. BAGDOYAN. Yes, sir.

Mr. HIGGINS. Isn't it true that a deranged individual wandered around the Boulder, Colorado, NIST campus and required medical attention because he accessed an area which houses toxic chemicals?

Mr. BAGDOYAN. That's my understanding of the incident. I don't know whether he was deranged or not but he certainly didn't belong where he was.

Mr. HIGGINS. Is the Boulder facility fenced?

Mr. BAGDOYAN. It is not.

Mr. HIGGINS. Thank you. Were there any mechanisms in place to warn the guards that this individual was present, an alarm system or something of that nature?

Mr. BAGDOYAN. I don't know.

Mr. HIGGINS. Did the folks on the ground at Boulder know how long this gentleman, what was the duration of time that he wandered undetected?

Mr. BAGDOYAN. I don't know, Mr. Higgins.

Mr. HIGGINS. Mr. Chairman, we have reviewed videos of the GAO undercover staff conducting testing of the physical security of these campuses, and I respectfully submit that the Department has considered this sensitive information and not appropriate for the public to see. But as an experienced former law enforcement officer, these videos do show evidence of repetitive failures of the security in place at these facilities and the need for substantial improvement from NIST and the Department, and I respectfully submit that these videos should be made public so that NIST be held accountable by the broader public, by we, the people, and by the taxpayers that we represent as opposed to just the members of this Committee, and with that, I respectfully yield back, Mr. Chairman.

Chairman LAHOOD. Thank you, Mr. Higgins, for your questions, and I think that concludes all the questions from Committee members at this time.

Let me just in closing thank you for being here and for your valuable testimony. I think collectively both Republicans and Democrats here today have expressed concern for what went on here with these three breaches and are going to be watching and monitoring to make sure that the implementation of the suggestions are put through and that we do everything we can to make sure that these facilities are secure and safe moving forward.

I would also ask that there was a number of requests made by members here today, that those be followed up by the witnesses. The record will remain open for two weeks for additional comments and written questions from members.

Pursuant to House Rule 11(g)(2) and the previous vote of the Subcommittees, the remainder of the hearing will be closed to the public because of the disclosure of the testimony that may be heard may compromise sensitive law enforcement information. The clerk will clear the room. Only Members of Congress, their staff, and witnesses may remain in the room. Once that's done, we'll begin the executive session.

[Whereupon, at 11:24 a.m., the Subcommittees proceeded in closed session.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Ms. Lisa Casias and Dr. Kent Rochford

House Committee on Science, Space, and Technology
Subcommittee on Oversight
Responses to Questions Submitted by Rep. Ed Perlmutter

1. **Can you please detail what physical security upgrades have been identified as options to better secure the Boulder Campus along with their approximate costs?**

   Upgrades:

   (1) Obtain equipment and services to replace or repair within 24 hours any critical security system component at the National Institute for Standards and Technology (NIST) Boulder that becomes inoperable (estimated cost $80,000). This activity will bring NIST Boulder into compliance with the ISC's Risk Management Process standard.

   (2) Modify or replace perimeter doors and door locks, emergency exit doors, operable ground floor windows, and windows within 16 feet of the ground or access point (estimated cost $1,300,000+).

   (3) Install cypher locks on laboratory doors (50-lock pilot project) (estimated cost $115,000).

   (4) Establish and implement security plans for construction and renovation projects (existing resources).

   (5) Implement baseline security requirements and accountability for all staff to prevent unauthorized access of NIST facilities (existing resources).

   a. **Which of these options can be funded through NIST and DOC's FY18 Budget Request?**

      Upgrades (1), (3), (4), and (5).

   b. **What other upgrades are planned for FY19 and beyond?**

      The Department of Commerce, Office of Security (OSY), will be conducting a campus Facility Security Assessment (FSA) in Boulder in FY18. The results will feed into plans for security upgrades in FY19 and beyond.

2. **What specific steps have been taken over the past several years and since the GAO investigation to improve collaboration with the security of other DoC agencies on the Boulder Campus?**

   The Board of Directors (BoD) for the Department's Boulder Laboratories has discussed and coordinated regularly on security matters prior to the Government Accountability

Office (GAO) review. The BoD includes representation from NIST, National Oceanic and Atmospheric Administration (NOAA), OSY, and the National Telecommunications and Information Administration (NTIA), all of whom operate laboratories at the Boulder campus.

The OSY Directors of Security at NIST, and NOAA, routinely travel to the Department's Boulder campus to meet with stakeholders, including members of the BoD. They also meet with the Federal Protective Service (FPS) Inspector assigned to the Boulder campus and the FPS Regional and District Commanders. FPS provides physical security for the Skaggs building (NOAA occupancy), though not for the other buildings on the Boulder campus.

The onsite (Boulder) OSY Deputy Chief of the Police Services Group (PSG) attends all quarterly BoD meetings, as well as monthly security meetings related to the Skaggs building held with NOAA and FPS.

OSY interviewed NIST, NOAA, and NTIA as part of the 2015 Anti-Terrorism Risk Assessments.

Since the release of the GAO report on October 11, 2017:

- The representatives of OSY, NIST, NOAA, and NTIA have met several times to discuss security matters and improve collaboration.
- NIST has shared its baseline security requirements, Frequently Asked Questions, and training with OSY, NOAA and NTIA.
- NIST, OSY, NOAA, and NTIA developed a brochure on safety and security for visitors to the DoC Boulder Laboratories.[1]
- OSY representatives met with NIST, NTIA, NOAA, General Services Administration (GSA), and the FPS representatives to ensure complete involvement in the upcoming FY18 Boulder campus FSA and began discussions on creating a campus Facility Security Committee (FSC) outside the BoD.

[1] NIST and OSY have developed a similar brochure for the Gaithersburg campus.

Responses by Mr. Seto Bagdoyen

Additional Material for the Record (QFRs)

Subcommittee on Oversight
Committee on Science, Space & Technology

Subcommittee hearing:
"FDIC Data Breaches:
Can Americans Trust that Their Private Banking Information Is Secure?"

October 26, 2017

Submitted by Mr. Seto Bagdoyan
Director, Audit Services
Government Accountability Office

Follow up from question regarding excluding personnel from GAO survey:

As indicated in our reports and written testimony, our survey sample included only scientific and technical personnel. We excluded administrative personnel because they may have varying levels of access and work in different capacities than the scientific and technical staff. For example, administrative personnel may not have the same level of access to restricted areas, such as laboratories, or equipment and materials that the scientific and technical personnel access on a regular basis.

○