BOLSTERING THE GOVERNMENT'S CYBERSECURITY: A SURVEY OF COMPLIANCE WITH THE DHS DIRECTIVE

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

November 14, 2017

Serial No. 115–38

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
27–677PDF WASHINGTON : 2018

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
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
RALPH NORMAN, South Carolina

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
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
BARRY LOUDERMILK, Georgia
ROGER W. MARSHALL, Kansas
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
LAMAR S. SMITH, Texas

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

CONTENTS

November 14, 2017

BOLSTERING THE GOVERNMENT'S CYBERSECURITY: A SURVEY OF COMPLIANCE WITH THE DHS DIRECTIVE

Tuesday, November 14, 2017

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

The Subcommittee met, pursuant to call, at 10:08 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Darin LaHood [Chairman of the Subcommittee] 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

Subcommittee on Oversight

Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive

Tuesday, November 14, 2017
10:00 a.m.
2318 Rayburn House Office Building

Witnesses

Ms. Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security

Ms. Renee Wynn, Chief Information Officer, National Aeronautics and Space Administration

Ms. Essye Miller, Deputy Chief Information Officer for Cybersecurity, U.S. Department of Defense

Dr. Mark Jacobson, Associate Teaching Professor, Edmund Walsh School of Foreign Service, Georgetown University

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

HEARING CHARTER

November 14, 2017

TO: Members, Subcommittee on Oversight

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

SUBJECT: Oversight Subcommittee hearing: *Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive*

The Subcommittee on Oversight will hold a hearing titled *Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive* on Tuesday, November 14, 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 and assess the implementation of the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 17-01 by federal government departments and agencies. The BOD requires federal government departments and agencies identify Kaspersky Lab software on their systems, take action to remove the software, and report to DHS. Witnesses will discuss federal IT procurement data and the process of identifying and removing software from federal systems, including potential solutions necessary for federal agencies to fortify IT systems.

Witness List:

- **Ms. Jeanette Manfra**, Assistant Secretary for Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security
- **Ms. Renee Wynn**, Chief Information Officer, National Aeronautics and Space Administration
- **Ms. Essye Miller**, Deputy Chief Information Officer for Cybersecurity, U.S. Department of Defense
- **Dr. Mark Jacobson**, Associate Teaching Professor, Edmund Walsh School of Foreign Service, Georgetown University

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. Good morning. The Subcommittee on Oversight will come to order.

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

Welcome to today's hearing entitled "Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive." The subject of today's hearing involves some information that is classified. I remind members that their questions may call for a response that the witnesses know to be classified. Please be mindful of this fact. I would like to instruct the witness to answer to the best of their ability, but should an answer call for sensitive information, members will understand if you respond that you are unable to answer in this setting.

I now recognize myself for five minutes for an opening statement.

Good morning and welcome to today's Oversight Subcommittee hearing, "Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive." The purpose of this hearing is to examine and assess implementation of the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 17–01, which was the removal of the Kaspersky-branded products by federal government departments and agencies.

This hearing marks the second time the Committee has convened to examine the issues and concerns surrounding Kaspersky Lab. On October 25, 2017, the Committee examined the potential risks, vulnerabilities, and threats posed to federal ICT systems by Kaspersky software. During that hearing, we heard from experts about the specific nature of threats posed by Kaspersky, action the federal government has taken or plans to take to mitigate the threat, and steps that could be taken to avoid similar threats in the future.

The Trump Administration has taken steps to remediate the Kaspersky issue. In July of this year, the GSA removed Kaspersky from its government-wide contracts. Although it was a step in the right direction, it did not completely eliminate the threat.

On September 13, 2017, the Administration took additional steps to harden the security of federal information systems against the Kaspersky threat when DHS issued Binding Operational Directive 17–01. The directive requires federal departments and agencies to complete three consecutive phases of implementation. First, they must scan their systems to identify the use or presence of Kaspersky software. Second, they must develop an action plan for the removal and replacement of any Kaspersky software identified on their systems. Finally, they are required to implement their action plan and must begin the process of removal and replacement.

Federal departments and agencies are also required to submit status reports to DHS as they implement each of the directive's three phases. The status reports provide data and information that is useful for assessing compliance with the directive, and for quantifying the pervasiveness of Kaspersky installations across federal systems, the extent of threats posed by the software, and the complexities associated with complete removal.

Today, we will focus primarily on the status reports to guide our assessment of compliance with the directive. In doing so, we hope to learn whether agencies have complied with the first two phases

of the directive and whether any Kaspersky installations were found on federal systems. Additionally, we hope to understand more about the specific action plans for removal and replacement of any identified Kaspersky installations and DHS' anticipated timeline for full implementation of the directive. Finally, we hope to learn about the directive's applicability to federal contractors.

I want to thank Ms. Miller for being here to represent the Department of Defense. Annually, the DOD spends approximately $30 billion on information technology. We are interested in whether the directive applies to DOD's contractors and, if so, are they currently complying? If not, what must be done to ensure that contractors take appropriate action to mitigate the Kaspersky threat? I'm hopeful that our witnesses today can help us resolve these important questions and better understand the next steps that must be taken to ensure the integrity, resilience, and security of federal information systems.

Cybersecurity is a complex and evolving issue that affects U.S. national and economic security. We must remain diligent in our efforts to strengthen and secure federal systems, and our approaches to addressing cybersecurity issues must evolve to keep pace with everchanging threats. Bolstering the cybersecurity of federal information systems is among the Committee's top priorities, and I am hopeful that our efforts here today will take us one step closer toward accomplishing this objective.

[The prepared statement of Chairman LaHood follows:]

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

For Immediate Release
November 14, 2017

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

Statement from Darin LaHood (R-Ill.)

Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive

Chairman LaHood: Good morning and welcome to today's Oversight Subcommittee hearing: "Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive."

The purpose of this hearing is to examine and assess implementation of Department of Homeland Security (DHS) Binding Operational Directive 17-01, Removal of Kaspersky-Branded Products, by federal government departments and agencies.
This hearing marks the second time the committee has convened to examine the issues and concerns surrounding Kaspersky Lab.

On October 25, 2017, the committee examined the potential risks, vulnerabilities and threats posed to federal IT systems by Kaspersky software. During that hearing, we heard from experts about the specific nature of threats posed by Kaspersky, action the federal government has taken or plans to take to mitigate the threat and steps that could be taken to avoid similar threats in the future.

The Trump administration has taken steps to remediate the Kaspersky issue. In July of this year, the GSA removed Kaspersky from its government-wide contracts. Although this was a step in the right direction, it did not completely eliminate the threat.

On September 13, 2017, the administration took additional steps to harden the security of federal information systems against the Kaspersky threat when DHS issued Binding Operational Directive 17-01.

The directive requires federal departments and agencies to complete three consecutive phases of implementation. First, they must scan their systems to identify the use or presence of Kaspersky software. Second, they must develop an action plan for the removal and replacement of any Kaspersky software identified on their systems. Finally, they are required to implement their action plan, and must begin the process of removal and replacement.

Federal departments and agencies are also required to submit status reports to DHS as they implement each of the directive's three phases. The status reports provide data and information that is useful for assessing compliance with the directive, and for quantifying the pervasiveness of Kaspersky installations across federal systems, the extent of threats posed by the software and the complexities associated with complete removal.

Today, we will focus primarily on the status reports to guide our assessment of compliance with the directive. In doing so, we hope to learn whether agencies have complied with the first two phases of the directive, and whether any Kaspersky installations were found on federal systems.

Additionally, we hope to understand more about the specific action plans for removal and replacement of any identified Kaspersky installations, and DHS' anticipated timeline for full implementation of the directive.

Finally, we hope to learn about the directive's applicability to federal contractors. I want to thank Ms. Miller for being here to represent the Department of Defense. Annually, DOD spends approximately $30 billion on information technology. We are interested in whether the directive applies to DOD's contractors and, if so, are they complying? If not, what must be done to ensure that contractors take appropriate action to mitigate the Kaspersky threat?

I'm hopeful that our witnesses today can help us resolve these important questions, and better understand the next steps that must be taken to ensure the integrity, resilience and security of federal information systems.

Cybersecurity is a complex and evolving issue that affects U.S. national and economic security. We must remain diligent in our efforts to strengthen and secure federal systems, and our approaches to addressing cybersecurity issues must evolve to keep pace with ever-changing threats.

Bolstering the cybersecurity of federal information systems is among the committee's top priorities, and I am hopeful that our efforts here today will take us one step closer toward accomplishing this objective.

###

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

Mr. BEYER. Thank you, Chairman LaHood, and thank you for holding this second hearing on Kaspersky.

Two weeks ago we held a hearing on security concerns regarding the use of Kaspersky Lab software on federal computer networks, and I think most members on both sides of the aisle agree that using the services or software of Kaspersky Lab, a Moscow-based company that reportedly has close ties to Russian intelligence services, using this on federal networks presents risks not worth taking.

So back in September, the Department of Homeland Security also recognized this and issued a directive for federal agencies to identify and initiate actions to remove Kaspersky Lab software from their networks. So I understand that we're holding this hearing as a follow-up to ensure that our federal agencies are complying with this DHS directive in a timely manner, which is essentially important.

However, it seems that in holding a second oversight hearing solely on Kaspersky Lab products we're missing the forest for the trees. Kaspersky products are not the biggest security risk we face in Russia. As I mentioned at our last hearing and as we saw throughout the 2016 election cycle, cybersecurity is no longer just about defending our data. It is on a larger scale about defending our democracy from unwanted foreign influence and disinformation campaigns.

Please listen to these actual numbers. One hundred and twenty-six million Americans received Russian-backed content on their Facebook newsfeeds during the 2016 election. Twitter has found 36,746 bots linked to Russia, and these accounts sent a combined 1.4 million tweets and were seen 288 million times. Google has uncovered tens of thousands of ads purchased by Kremlin-linked buyers on YouTube, Gmail—its search page—and in double-click ads. The Kremlin directly sponsored fake Black Lives Matter activists who posted videos to Facebook, Twitter, and YouTube. Last month, the Computational Propaganda Project released a study mapping how Russia-linked Twitter accounts seek to target U.S. military personnel and veterans.

So instead of focusing just on Kaspersky Lab software, we should also be examining how enemies of democracy are using communications technologies in new, precise, and powerful ways to disrupt our democratic institutions and influence the American public. We should be specifically looking into how the Russians have done this just during the 2016 presidential election and how we can develop tools, technologies, and public awareness to diminish similar attacks in the future. We should also examine the state of our cybersecurity practices in defending our critical election infrastructure from covert interference and manipulation.

The House Science, Space, and Technology Committee has an important role in publicly addressing these issues. We do have a specific responsibility to provide oversight on the deeply existential role of technology in our society. And, Mr. Chairman, at the last Kaspersky hearing I requested that we hold a hearing on these larger issues, and I respectfully ask again today.

I'm glad that one of our witnesses today will help put the security concerns regarding Kaspersky Lab's software in context and helps examine the broader Russian strategy of undermining our democratic institutions and influencing our democracy. Dr. Mark Jacobson, a professor at Georgetown University, has written frequently on the impact of Russia's influence operations against the United States in the past few years. I look forward to his testimony and all your testimony.

I'm also attaching to my statement a minority staff report that addresses Russia's cyber influence campaign against the United States. This report has already been shared with the majority staff.

Thank you, Mr. Chairman, and I yield back.

[The prepared statement of Mr. Beyer follows:]

OPENING STATEMENT
Ranking Member Donald S. Beyer, Jr. (D-VA)
of the Subcommittee on Oversight

Committee on Science, Space & Technology
"Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive"
November 14, 2017

Thank you, Chairman LaHood. Three weeks ago we held a hearing on security concerns related to the use of Kaspersky Lab software on federal computer networks. I think most Members across the aisle agreed that using the services or software of Kaspersky Lab, a Moscow-based company that reportedly has close ties to Russian intelligence services, on federal networks presents risks not worth taking. Back in September, the Department of Homeland Security also recognized this, and issued a directive to federal agencies to identify and initiate actions to remove Kaspersky Lab software from their networks.

I understand that we're holding this hearing as a follow-up to ensure that our federal agencies are complying with the DHS directive in a timely manner, which is important given the grave risks. However, it seems that in holding a second oversight hearing on ***solely*** Kaspersky Lab products, we're missing the forest for the trees. Kaspersky products are not ***the*** biggest security risk we face from Russia. As I mentioned at our last hearing, and as we saw throughout the 2016 election cycle, cybersecurity is no longer just about defending our data—it is, on a larger scale, about defending our democracy from unwanted foreign influence and disinformation campaigns.

Instead of focusing just on Kaspersky Lab software, we should be examining how enemies of democracy are using communication technologies in new, precise and powerful ways to disrupt our democratic institutions and influence the American public. We should be specifically looking into how the Russians have done just this during the 2016 U.S. Presidential Election and how we can develop tools, technologies, and public awareness to diminish similar attacks in the future. We should also examine the state of our cyber security practices in defending our critical election infrastructure from covert interference and manipulation. The House Science Committee has an important role in publicly addressing these issues. Mr. Chairman, at the last Kaspersky hearing, I requested that you hold a hearing on these larger issues, but I am asking once again today.

I am glad that at least one of our witnesses today will help put the security concerns regarding the use of Kaspersky Lab software in context and help us examine the broader Russian strategy of undermining our democratic institutions and influencing our democracy. Dr. Mark Jacobson, a professor at Georgetown University, has written frequently on the impact of Russia's influence operations against the United States in the past few years. I look forward to his testimony.

I welcome all of our witnesses to today's hearing. I am also attaching to my statement a Minority Staff Report that addresses Russia's cyber influence campaign against the U.S. This report has already been shared with the Majority staff.

Thank you, Mr. Chairman. I yield back.

Chairman LAHOOD. Thank you, Mr. Beyer.

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

Chairman SMITH. Thank you, Mr. Chairman.

The risk to U.S. security that Kaspersky Lab, a Russian company, has created is undeniable and the harm, incalculable. The founder of Kaspersky Lab, Eugene Kaspersky, attended a KGB-funded intelligence institute and served in Russia's Ministry of Defense. For years, there has been speculation that Kaspersky's antivirus software could be used by the Russians for information gathering. Continued investigations have disclosed more details on the extent to which Kaspersky Lab is a tool for the Russian Government. Press reports claim that Kaspersky's prior federal government customers include the Departments of State, Justice, Energy, Defense, Treasury, Army, Navy and Air Force. This is of more than passing concern; it is alarming.

Last month, The New York Times reported that Russian Government hackers conducted a global search of computers looking for the code names of American intelligence programs. The hackers used the antivirus software made by Kaspersky Lab. This Russian operation stole classified documents from at least one National Security Agency employee, who had Kaspersky antivirus software installed on his home computer.

Kaspersky's antivirus software allowed Russia to have unlimited access to data stored on computers with Kaspersky products. The magnitude and widespread use of Kaspersky's software—400 million users worldwide—gives the company unprecedented access and retrieval capabilities.

To date, it is unclear what additional American security secrets Russia may have acquired through Kaspersky's scans for classified programs. This only confirms the need for the actions this Administration and this Committee have taken. The Science Committee has engaged in continued oversight of Kaspersky Lab since questions were raised by Science Committee member Congressman Higgins earlier this year. On July 27, 2017, this committee requested that all federal departments and agencies disclose their use of Kaspersky Lab products. On September 13, 2017, the Department of Homeland Security issued a Binding Operational Directive to all agencies and departments. This directive sought the complete removal of Kaspersky products from federal systems after 90 days.

Today, the Committee is interested in whether federal agencies are complying with the directive. How common are Kaspersky products in our federal systems? What is the extent of the risk? And are the actions required in the DHS directive sufficient to protect U.S. interests? The Committee expects to uncover all risk associated with Kaspersky Lab. This includes identifying all necessary actions needed to eliminate risks even beyond the risk to federal systems.

Based on the NSA contractor's personal computer being targeted, we are interested in what steps DHS has taken to assist civilian employees and contractors who are at risk of exposure. We also are interested in proactive steps and coordination among our federal agencies and departments. We need to use all resources to ensure

that Kaspersky products on federal systems have been completely removed.

Beyond an interest in the risk caused by Kaspersky products, the Science Committee will continue to address the federal government's cybersecurity weaknesses.

This committee, along with the Committee on Oversight and Government Reform, plans to bring a revised version of H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, to the House Floor soon. NIST should welcome the opportunity to use its expertise to help protect our national security.

The bill amends the Federal Information Security Management Act to require that federal agencies' Inspectors General coordinate with NIST in conducting their cybersecurity evaluations. Anyone with knowledge of potential cybersecurity risks should contact the committee and share their information with us. We must eliminate the threat of Kaspersky Lab to our national security systems. 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
November 14, 2017

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

Statement from Lamar Smith (R-Texas)

Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive

Chairman Smith: The risk to U.S. security that Kaspersky Lab, a Russian company, has created is undeniable and the harm, incalculable.

The founder of Kaspersky Lab, Eugene Kaspersky, attended a KGB-funded intelligence institute and served in Russia's Ministry of Defense.

For years there has been speculation that Kaspersky's antivirus software could be used by the Russians for information gathering.

Continued investigations have disclosed more details on the extent to which Kaspersky Lab is a tool for the Russian government.

Press reports claim that Kaspersky's prior federal government customers include the departments of State, Justice, Energy, Defense, Treasury, Army, Navy and Air Force. This is of more than passing concern; it is alarming.

Last month, The New York Times reported that Russian government hackers conducted a global search of computers looking for the code names of American intelligence programs. The hackers used the antivirus software made by Kaspersky Lab.

This Russian operation stole classified documents from at least one National Security Agency employee, who had Kaspersky antivirus software installed on his home computer.

Kaspersky's antivirus software allowed Russia to have unlimited access to data stored on computers with Kaspersky products. The magnitude and widespread use of Kaspersky's software – 400 million users worldwide – gives the company unprecedented access and retrieval capabilities.

To date, it is unclear what additional American security secrets Russia may acquired through Kaspersky's scans for classified programs. This only confirms the need for the actions this administration and this committee have taken.

The Science Committee has engaged in continued oversight of Kaspersky Lab since questions were raised by Science Committee member Congressman Higgins earlier this year.

On July 27, 2017, this committee requested that all federal departments and agencies disclose their use of Kaspersky Lab products.

On September 13, 2017, the Department of Homeland Security issued a Binding Operational Directive to all agencies and departments. This directive sought the complete removal of Kaspersky products from federal systems within 90 days.

Today, the committee is interested in whether federal agencies are complying with the directive. How common are Kaspersky products in our federal systems? What is the extent of the risk? And are the actions required in the DHS directive sufficient to protect US interests?

The committee expects to uncover all risks associated with Kaspersky Lab. This includes identifying all necessary actions needed to eliminate risks even beyond the risk to federal systems.

Based on the NSA contractor's personal computer being targeted, we are interested in what steps DHS has taken to assist civilian employees and contractors who are at risk of exposure.

We also are interested in proactive steps and coordination among our federal agencies and departments. We need to use all resources to ensure that Kaspersky products on federal systems have been completely removed.

Beyond an interest in the risks caused by Kaspersky products, the Science Committee will continue to address the federal government's cybersecurity weaknesses.

This committee, along with the Committee on Oversight and Government Reform, plans to bring a revised version of H.R. 1224, the NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017, to the House floor soon. NIST should welcome the opportunity to use its expertise to help protect our national security.

The bill amends the Federal Information Security Management Act to require that federal agencies' inspectors general coordinate with NIST in conducting their cybersecurity evaluations.

Anyone with knowledge of potential cybersecurity risks should contact the committee and share their information with us.

We must eliminate the threat of Kaspersky Lab to our national security systems.

###

Chairman LAHOOD. Thank you, Chairman Smith.

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

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

In September, the Department of Homeland Security banned the use of Kaspersky Lab software on federal government computer networks. The U.S. intelligence community believes this Russian company's products pose an unnecessary potential risk to our security from Russia's intelligence services. Whether or not the company is aware of these threats is irrelevant. I trust the judgment of the American intelligence community in this matter, and I'm also confident that federal agencies will successfully eliminate the Kaspersky Lab software from their respective computer systems.

I am much more concerned, though, about the persistent threat foreign actors pose to our electoral system. During the previous Kaspersky Lab hearing the Subcommittee held three weeks ago, I noted that, prior to the 2016 election, this committee held a hearing to review the guidelines for protecting voting and election systems, including voter registration databases and voting machines. I asked that this committee hold a follow-up hearing to discuss protecting these same systems in the light of last year's events, as well as to examine the sophisticated influence operations conducted by the Russian Intelligence Service to disrupt our democratic processes and damage our democracy.

Today, I want to reiterate that request. Russian actors attempted to hack into voter databases in multiple States before the 2016 election, successfully compromising a small number of networks according to the Department of Homeland Security. But Russia, as we all know, did not only attempt to penetrate these sorts of hard targets, they sought to influence public opinion and undermine our democratic institutions through their use of trolls, bots, and social media platforms.

Rather than simply examine the specific threat posed by Kaspersky Lab software, we need to take a much wider view and look at the evolving and expanding threat that Russians' cyber attacks and influence operations pose today in our society.

I'm happy that Dr. Mark Jacobson, our witness today, can speak about Russia's history of influence operations against the United States and the many ways that Russia seeks to undermine Western democracies. I thank you for coming today, Dr. Jacobson.

I ask again for the Science Committee to commit to holding a 2016 election postmortem with an eye on ways the Science Committee can help discourage foreign interference in future elections and how we can encourage the development of tools and technologies to help identify these threats and limit their impact on our government, public, and society.

I thank you, Mr. Chairman, and I yield back the balance of my time.

[The prepared statement of Ms. Johnson follows:]

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

Committee on Science, Space, and Technology
Subcommittee on Oversight
"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"
November 14, 2017

Thank you Chairman LaHood.

In September, the Department of Homeland Security banned the use of Kaspersky Lab software on federal government computer networks. The U.S. intelligence community believes this Russian company's products pose an unnecessary potential risk to our security from Russia's intelligence services. Whether or not the company is aware of those threats is irrelevant. I trust the judgment of the American intelligence community in this matter. I am also confident that federal agencies will successfully eliminate Kaspersky Lab software from their respective computer systems. I am much more concerned, though, about the persistent threat foreign actors pose to our electoral system.

During the previous Kaspersky Lab hearing the Subcommittee held three weeks ago, I noted that prior to the 2016 Election, this Committee held a hearing to review the guidelines for protecting voting and election systems—including voter registration databases and voting machines. I asked that this Committee hold a follow-up hearing to discuss protecting these same systems, in the light of last year's events, as well as to examine the sophisticated influence operations conducted by Russian intelligence services to disrupt our democratic processes and damage our democracy. Today I want to reiterate that request.

Russian actors attempted to hack into voter databases in multiple states before the 2016 election, successfully compromising "a small number of networks," according to the Department of Homeland Security. But Russia, as we all know, did not only attempt to penetrate these sorts of hard targets, they sought to influence public opinion and undermine our democratic institutions through their use of trolls, bots and social media platforms. Rather than simply examine the specific threat posed by Kaspersky Lab software, we need to take a much wider view and look at the evolving and expanding threat that Russian cyber attacks and influence operations pose today in our society. I am happy that Dr. Mark Jacobson, our witness today, can speak about Russia's history of influence operations against the United States and the many ways that Russia seeks to undermine Western democracies. Thank you for coming today Dr. Jacobson.

I again ask for the Science Committee to commit to holding a 2016 Election post mortem, with an eye on ways the Science Committee can help discourage foreign interference in future elections and how we can encourage the development of tools and technologies to help identify these threats and limit their impact on our government, public and society.

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

Chairman LAHOOD. Thank you, Ms. Johnson.

At this time let me introduce our witnesses here today. Our first witness today is Ms. Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate at the U.S. Department of Homeland Security. Ms. Manfra has held multiple positions related to cybersecurity at the Department, and prior to serving at DHS, Ms. Manfra served in the U.S. Army as a Communications Specialist and a Military Intelligence Officer. Welcome.

Our second witness is Ms. Reñe Wynn, Chief Information Officer at NASA. Ms. Wynn previously served as the Acting Assistant Administrator for the Office of Environment Information at the EPA. She holds a bachelor of arts in economics from DePauw University in Indiana. Welcome, Ms. Wynn.

Our third witness is Ms. Essye Miller. She is the Deputy Chief Information Officer for Cybersecurity at the U.S. Department of Defense. Ms. Miller previously served as the Director of Cybersecurity for the Army Chief Information Officer. She received her bachelor's degree from Talladega College and a master's from Troy State University, as well as from Air University at the Air War College. Welcome.

Our last witness today is Dr. Mark Jacobson. He is an Associate Teacher Professor for the Edmund Walsh School of Foreign Service at Georgetown University. Dr. Jacobson previously held appointments as a Senior Advisor to the Secretary of Defense and as a Special Assistant to the Secretary of the Navy. He has also served as the Deputy NATO Representative and Director of International Affairs at the International Security Assistance Force. Dr. Jacobson holds degrees from the University of Michigan, the King's College, University of London, and a Ph.D. in military history from Ohio State University. Welcome.

At this time I now recognize Ms. Manfra for five minutes to present her testimony.

TESTIMONY OF MS. JEANETTE MANFRA,
ASSISTANT SECRETARY FOR CYBERSECURITY
AND COMMUNICATIONS,
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE,
U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. MANFRA. Thank you, sir. Mr. Chairman, Ranking Member Beyer, Mr. Smith, and Ranking Member Johnson, and members of the committee, today's hearing is an opportunity to discuss the Department of Homeland Security's actions regarding Kaspersky Lab products. As the Assistant Secretary for Cybersecurity and Communications, I lead many of the Department's efforts to safeguard and secure cyberspace, a core homeland security mission. We work every day to protect federal government agencies and collaborate with state, local, tribal, and territorial governments and the private sector to enhance the security and resilience of our cyber and physical infrastructure.

Earlier this year, the President signed an executive order on strengthening the cybersecurity of federal networks and critical infrastructure. This executive order set in motion a series of assess-

ments and deliverables to improve our defenses and lower our risk to cyber threats. DHS has organized around these deliverables by working with government and private sector partners.

Federal agencies have been implementing the NIST cybersecurity framework. Agencies are reporting to DHS and the Office of Management and Budget on their cybersecurity risk mitigation and acceptance choices. DHS and OMB are evaluating the totality of these agency reports in order to comprehensively assess the adequacy of the federal government's overall cybersecurity risk management posture.

In addition to our efforts to protect government networks, we are focused on how government and industry work together to protect the Nation's critical infrastructure. We are prioritizing deeper more collaborative public-private partnerships.

Protecting federal information systems requires addressing risks within supply chain. The Department has been actively engaged in its own efforts, as well as broader interagency efforts to address IT supply chain threats. As we build on best practices to improve the federal government's own actions within this space, we will coordinate and share information with our state and local government partners, as well as the private sector critical infrastructure community.

Among other authorities, the Federal Information Security Modernization Act of 2014, commonly referred to as FISMA, authorizes the Department of Homeland Security to develop and oversee the implementation of binding operational directives, or BODs. These directives to federal agencies are for purposes of safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk. Federal agencies are required to comply with these DHS-developed directives.

On September 13 of this year DHS's Acting Secretary signed a binding operational directive to address the use or presence of Kaspersky Lab products, solutions, and services on federal information systems. After careful consideration of available information and consultation with interagency partners, DHS determined Kaspersky Lab products present a known or reasonably suspected information security risk to federal information systems. In a public statement, the Department identified concerns regarding, one, the ties between certain Kaspersky officials and Russian intelligence and other government officials; two, the requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks; and three, the broad access to files and elevated privileges provided by antivirus products and services, including Kaspersky products, that can be exploited by malicious cyber actors to compromise information systems. The action taken is a reasonable, measured approach to the information security risks posed by these threats—or posed by these products to the federal government.

In addition to the reports from agencies required by this directive, our National Cybersecurity and Communications Integration Center continues to operate important capabilities that help DHS better understand the use of these products within the federal gov-

ernment. For instance, we operate capabilities that monitor NetFlow at federal agencies commonly referred to as Einstein. We also provide agencies tools within our Continuous Diagnostics and Mitigation program. Both of these capabilities enabled us to further our understanding of the presence of Kaspersky products on agency networks.

I want to thank Congress for your focus on these issues and highlighting the concerns here. Your focus has been extremely helpful to us as we have evaluated the evidence, communicated with our colleagues around the interagency, and made the decision to issue the binding operational directive.

It is important for the committee to understand that DHS is providing an opportunity for Kaspersky and any other entity that claims its commercial interests will be directly impacted to submit a written response and any additional information or evidence. DHS will review any submissions closely and make adjustments to a directive—to our directive if appropriate.

Before closing, I want to assure the Committee that I will answer your questions to the extent I can in an open hearing and at this time. Some of your questions may require the discussion of classified information, which I clearly cannot address in an open hearing. Other questions may not be appropriate to address at this time because we are in the middle of an administrative process with the affected entity, and there could be litigation related to this directive. Because we need to provide the company with a meaningful opportunity to be heard, and there may be federal court review of our actions and decisions, there may be certain issues that it would not be appropriate for me to comment on until the conclusion of this administrative process.

Thank you very much for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Ms. Manfra follows:]

Written Testimony

Jeanette Manfra
Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
U.S. House of Representatives
House Committee on Science, Space, and Technology
Oversight Subcommittee

Implementation of the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 17-01 - Kaspersky Lab Software

November 14, 2017

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for your interest in this important issue and the opportunity to provide an update on the Department's position regarding the Federal government's use of Kaspersky Lab (KL) software. I am the Assistant Secretary for Cybersecurity and Communications within the DHS National Protection and Programs Directorate (NPPD). NPPD executes many of the Department's authorities related to cybersecurity of federal networks.

The Federal Information Security Modernization Act of 2014 (FISMA) authorizes DHS to develop and oversee the implementation of binding operational directives (BODs), that are consistent with Office of Management and Budget (OMB) policies as well as National Institute of Standards and Technology (NIST) standards, to federal departments and agencies. FISMA defines a BOD as a "compulsory direction to an agency that is for purposes of safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk." Federal agencies are required to comply with these DHS-developed directives.

A priority of DHS is to ensure the integrity and security of U.S. government systems, and in doing so must safeguard federal government systems by reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats.

On September 13, 2017, DHS Acting Secretary Elaine Duke signed BOD 17-01 to address the use of Kaspersky products, solutions, and services on federal information systems. After consultation with interagency partners, DHS determined Kaspersky products present a known or reasonably suspected information security risk to federal information systems. The BOD directs agencies to identify the use of these products within 30 days, provide a plan to remove them within 60 days, and, unless directed otherwise by DHS based on new information, to begin removing products at 90 days.

The Secretary's decision to issue the BOD is based on expert judgments about risks to federal information and information systems, which directly impact U.S. national security. In a public statement, the Department explained that it is concerned about (1) the ties between certain Kaspersky officials and Russian intelligence and other government agencies, (2) requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks, and (3) the broad access to files and elevated privileges provided by anti-virus products and services, including Kaspersky products, that can be exploited by malicious cyber actors to compromise information systems. The decision to use an anti-virus product is an information security risk decision ultimately based in trust. Given the ties between the company and Russian government agencies, the structure of the law in Russia, and the broad access that these products and services have, the Department lacks the necessary trust to allow the deployment of these products and services on

federal information systems. The action taken is a reasonable, measured approach to the information security risks posed by these products.

DHS is providing an opportunity for Kaspersky and any other entity that claims its commercial interests will be directly impacted by the BOD to submit to DHS a written response and any additional information or evidence supporting the response, to explain the adverse consequences, address the Department's concerns, or mitigate those concerns. DHS will review any submissions closely. As indicated in the BOD, DHS may provide other direction to federal agencies, based on new information, before the 90 day mark when agencies are to begin implementing the agency's plan of action to remove and discontinue use of Kaspersky products.

Thank you for the opportunity to testify today and I look forward to your questions.

Jeanette Manfra
Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Jeanette Manfra serves as the Assistant Secretary for the Office of Cybersecurity and Communications (CS&C). She is the chief cybersecurity official for the Department of Homeland Security (DHS) and supports its mission of strengthening the security and resilience of the nation's critical infrastructure.

Prior to this position, Ms. Manfra served as Acting Deputy Under Secretary for Cybersecurity and Director for Strategy, Policy, and Plans for the NPPD.

Previously, Ms. Manfra served as Senior Counselor for Cybersecurity to the Secretary of Homeland Security and Director for Critical Infrastructure Cybersecurity on the National Security Council staff at the White House.

At DHS, she held multiple positions in the Office of Cybersecurity and Communications, including advisor for the Assistant Secretary for Cybersecurity and Communications and Deputy Director, Office of Emergency Communications, during which time she led the Department's efforts in establishing the Nationwide Public Safety Broadband Network.

Before joining DHS, Jeanette served in the U.S. Army as a communications specialist and a Military Intelligence Officer.

Chairman LAHOOD. Thanks, Ms. Manfra.

At this time I now recognize Ms. Wynn for five minutes to present her testimony.

TESTIMONY OF MS. RENEE WYNN,
CHIEF INFORMATION OFFICER,
NATIONAL AERONAUTICS
AND SPACE ADMINISTRATION

Ms. WYNN. Great. Good morning, Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify before you today regarding NASA's efforts to comply with the recent Department of Homeland Security binding operational directive regarding Kaspersky-branded products.

As NASA's Chief Information Officer, my number-one priority is to effectively manage and protect NASA's information technology assets in an everchanging threat landscape. Each day, hundreds of thousands of NASA personnel, contractors, academics, international partners, and members of the public access some part of NASA's IT infrastructure, which is a complex array of information systems with more than 160,000 components geographically dispersed around the globe and beyond.

NASA works closely with our federal cybersecurity partners to ensure NASA's network is safeguarded from threats, assessed against stringent federal and agency security requirements, and continuously monitored for compromise and the effectiveness of our security measures.

New cybersecurity tools, particularly the Department of Homeland Security's Continuous Diagnostics and Mitigation program, are allowing us to have better insights into our networks, which allows us to better mitigate threats. However, given the evolving nature of threats, our work is never done.

Antivirus software is one component of endpoint protection implemented to safeguard NASA systems and data. NASA has been using Symantec Endpoint Protection software as its desktop standard load since 2010. Therefore, Kaspersky-branded products, the focus of today's hearing, are not part of NASA's standard load software.

Between January 1, 2013, and mid-August 2017, NASA identified a small number of machines which had Kaspersky-branded products preinstalled. When discovered, these instances were removed to comply with NASA's desktop standard software configuration. Another item of importance is that NASA's Office of Procurement has no record of NASA funds being used to purchase individual instances of Kaspersky-branded products. Therefore, we believe that the limited instances of Kaspersky-branded products found to exist on agency hardware were likely the result of larger procurements and bundled preinstalled software.

On September 13, 2017, NASA received the Binding Operational Directive 17–01, which required all federal executive branch departments and agencies to take action with regard to Kaspersky-branded products on federal IT systems. NASA notified the Department of Homeland Security on Friday, October 13, that no Kaspersky-branded products were identified on NASA systems.

Therefore, no additional actions are required by NASA under the terms of the binding operational directive.

Also of note, in 1993, the General Services Administration asked NASA to be part of a pilot project for the governmentwide acquisition contracts. Subsequently, NASA was one of three agencies designated to provide a governmentwide contract vehicle for other agencies to use when acquiring IT products and services for their own agencies. This vehicle is known at NASA as the Solutions for Enterprise-Wide Procurement or SEWP. In July 2017, in coordination with the General Services Administration, NASA removed all offerings of Kaspersky-branded products from the SEWP database and installed filters to prevent Kaspersky-branded products from being re-added.

In conclusion, protecting and upgrading and better managing NASA's IT infrastructure is and will remain a top agency priority. When threats such as unauthorized software are detected, NASA personnel take action. NASA is fully committed to becoming more secure, effective, and resilient, and we are actively pursuing this on all levels.

Thank you for the opportunity to testify before you today, and I'd be happy to answer any questions that you may have.

[The prepared statement of Ms. Wynn follows:]

HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
Nov. 14, 2017

Statement of
Reneé Wynn
Chief Information Officer
National Aeronautics and Space Administration

before the

Subcommittees on Oversight
Committee on Science, Space and Technology
U.S. House of Representatives

Chairman LaHood and Ranking Member Beyer, and Members of the Subcommittee, thank you for the opportunity to testify before you today regarding NASA's efforts to comply with a recent Binding Operational Directive (BOD) issued by the U.S. Department of Homeland Security (DHS) with regard to Kaspersky Lab-branded products. As NASA's Chief Information Officer (CIO), effectively managing and protecting the Agency's information technology (IT) resources in an ever-changing threat landscape is my number one priority.

Currently about 17,100 civil servants and 40,000 contractors work at nine NASA Centers and one Federally Funded Research and Development Center, as well as several smaller satellite facilities. We also collaborate with other international space agencies and have deep partnerships with researchers, engineers and scientists all over the world. Each day, hundreds of thousands of NASA personnel, contractors, academics and members of the public access some part of NASA's IT infrastructure – a complex array of information systems with more than 160,000 components geographically dispersed around the globe and beyond. This infrastructure plays a critical role in every aspect of NASA's mission, from controlling spacecraft to processing scientific data.

In support of NASA's many missions, the Office of the Chief Information Officer (OCIO) works to ensure that NASA's IT systems and their associated components are safeguarded from attack, assessed against stringent Federal and Agency security requirements, and are continuously monitored for compromise and for the effectiveness of currently implemented security measures. Given the evolving threat of attacks, our work is never done. Internal governance and infrastructure changes at NASA have already improved the Agency's security posture, but admittedly, more work remains, especially as the Agency evolves from a highly decentralized IT environment controlled by the Centers and Agency programs and projects to an enterprise IT environment that is more centrally managed and overseen by the Agency CIO.

NASA regularly conducts network scans on its internal, corporate network, mission operations networks, and provisioned guest networks. Corporate and mission networks are used to process Government data for official NASA business operations. Guest networks are for official, authorized NASA visitors and are not used to conduct NASA business or transmit Government data. NASA monitors systems connecting to its guest networks for improper use and malicious activity but it does not have complete insight into the system's hardware configurations or software inventory. To mitigate potential risk from these external systems, guest networks are designed as untrusted networks that have no privileged access to NASA data.

Additionally, the collective actions of NASA's OCIO, as well as information sharing with the DHS and other Federal agencies involved in cybersecurity, are contributing to an improved security posture. When threats are detected, NASA incident response personnel take immediate action, and depending on the level of the threat, NASA alerts other Federal agencies involved with cyber intelligence issues, and partners with them to deter and thwart future attacks.

Key Events

With regard to today's hearing topic, NASA would like to stress that Kaspersky Lab software is not part of the Agency's enterprise-licensed, core-load anti-virus software. Instead, since 2010, NASA has used Symantec Endpoint Protection as its core-load anti-virus solution under our End User Service contract. Therefore, the existence of any alternative anti-virus software on Agency hardware is considered to be a violation of Agency IT standards and will be immediately removed or its usage blocked unless a specific waiver is on file based on a risk assessment performed by the NASA OCIO -- the Agency's sole authority for NASA IT, to include IT risk acceptance.

Between Jan. 1, 2013 and mid-August 2017, NASA OCIO identified a small number of machines (work stations and mobile devices) which had Kaspersky Lab software installed on them and which were authorized to and did connect to NASA's internal network. This number included third-party international partners / bring your own device users. It is important to note that the NASA Office of Procurement has no record of Agency funds being used to purchase individual instances of Kaspersky Lab software, which leads officials to believe that the limited instances of Kaspersky Lab software found to exist on Agency hardware were likely the result of larger procurements and bundled services which included Kaspersky Lab software for free on purchased hardware. However, again, I must stress that the existence of Kaspersky Lab software or the existence of any non- Symantec anti-virus software on Agency hardware is a violation of Agency IT standards unless a waiver is granted by the CIO or her delegate.

On Sept. 13, 2017, NASA received DHS BOD-17-01 which required Federal and Executive branch departments and agencies to take action with regard to Kaspersky branded products on Federal IT systems. To comply with the BOD, departments and agencies were required to respond to DHS and to take specified actions within 30 and 60 days of, and at 90 days after, the BOD's issuance. Since receiving the BOD, NASA OCIO has identified no active installations of Kaspersky-branded products on devices or systems within the scope of BOD 17-01. NASA OCIO continues to leverage deployed continuous monitoring tools and regular incident response activities across NASA Centers to review and validate that Kaspersky Lab products are not appearing on the NASA network.

Also of note, in 1993, NASA was requested by the Government Services Agency (GSA) to be the pilot for the concept of Government-Wide Acquisition Contracts (GWAC). Subsequently, the Office of Management and Budget designated three agencies: NASA, the National Institutes of Health and GSA to provide GWAC vehicles for the use of acquiring IT products and services by the entire Federal Government. NASA's Solutions for Enterprise Wide Procurement (SEWP)[1] contract database then became the Agnecy's GWAC vehicle and as such supported acquisitions by NASA and the rest of the Federal Government. In July 2017, in coordination with the GSA and other major Government-wide contract vehicles, all offerings of Kaspersky Labs software were removed from NASA's SEWP contract

[1] The NASA SEWP Program Office operates under the Goddard Space Flight Center's CIO Office. Software and hardware is added by the various contract holders to provide the various Government agencies with offerings that the contract holders want to make available for purchase. There are currently 140 contract holders with products and services from 5500 manufacturers/software companies

database. Additionally Kaspersky Labs was de-activated as a legitimate provider for any future items being added to the SEWP contracts to avoid any possibility that items would be re-added later.

NASA Cybersecurity Environment

Before I conclude my testimony, I would like to speak briefly about NASA's cyber threat environment and our constant efforts to improve how we manage and protect our IT resources.

Decades of NASA aeronautics and space technology research and development represents billions of dollars in U.S. Government and aerospace industry investment. The very nature of NASA's mission, and the extremely important technical and intellectual capital produced therein, makes the Agency's information a valuable target for hackers, criminals and foreign enterprises. Many of these threats are well-resourced, highly motivated, and exhibit varying levels of sophistication. Therefore, there is no perfect, one-size-fits-all tool to predict, counter and mitigate the wide range of attacks across the Federal Government. However, new cybersecurity management tools are allowing NASA and other Federal agencies to have better insight into their networks, providing improved pro-active monitoring and mitigation of threats before they cause significant harm. For example, as part of NASA's implementation of the DHS Continuous Diagnostic Management (CDM) tool, NASA is transitioning in the near term to a unified vulnerability reporting dashboard structure. Full capability expected to be available in Fiscal Year 2018, as CDM phase 1 is completed in accordance with the DHS CDM implementation schedule. CDM Phase 1 will provide the following enhanced capabilities to the NASA continuous monitoring program:

- Hardware Asset Management: Using a tool to perform network discovery of all devices connected to any NASA owned or managed internet protocol address space, categorize the detected devices and monitor those devices;
- Software Asset Management: Using several tools to perform software inventory of all supported end-user devices, implement software whitelisting capability, monitor use of authorized and unauthorized software, and report software patch status for all supported end-user device;
- Configuration Settings Management: Using a tool to automate scanning of the U.S. Government Configuration Baseline and NASA configuration baseline settings and to decrease the time to scan for vulnerabilities; and
- Vulnerability Management: Using a tool establish configuration policies and automate network vulnerability scanning, and using the CDM Dashboard to enhance visibility.

Conclusion

In conclusion, protecting, better managing and upgrading NASA's IT infrastructure is and will remain a top Agency priority. When threats such as unauthorized software are detected, NASA personnel take immediate action to contain the threat. NASA is fully committed to becoming more secure, effective and resilient, and we are actively pursuing this on all levels.

Thank you for the opportunity to testify before you today, and I would be happy to answer any questions that you may have.

Reneé P. Wynn
NASA's Chief Information Officer

Reneé P. Wynn is the NASA Chief Information Officer. Wynn joined NASA in July 2015 as the Deputy Chief Information Officer. She came to NASA from the Environmental Protection Agency (EPA) where she had served as the Acting Assistant Administrator for the Office of Environmental Information since July 2013. Ms. Wynn has a long career in the Federal government. She was with EPA for more than 25 years, and joined the Office of Environmental Information in April 2011. Beyond the experience she gained since joining the information management and technology arm of the Agency, Ms. Wynn served in EPA's Office of Solid Waste and Emergency Response and the Office of Enforcement and Compliance Assurance.

Ms. Wynn has managed program administration for science, information management, and international programs; regulatory management; budget formulation and execution; contracts, grants and interagency agreements; long term strategic planning and analyses; and environmental and administrative policy.

Ms. Wynn holds a Bachelor of Arts in Economics from DePauw University, Indiana.

Chairman LAHOOD. Thank you, Ms. Wynn.

At this time, I recognize Ms. Miller for five minutes for her testimony.

TESTIMONY OF MS. ESSYE MILLER,
DEPUTY CHIEF INFORMATION OFFICER
FOR CYBERSECURITY, U.S.
DEPARTMENT OF DEFENSE

Ms. MILLER. Good morning, Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify today on the Department of Defense position regarding the federal government's use of Kaspersky Lab software.

I currently serve as the Deputy Chief Information Officer for Cybersecurity at the Department of Defense. Additionally, I serve as the Department's Chief Information Security Officer. My primary responsibility is to ensure that the Department has a well-defined and executed cybersecurity program. I am also responsible for coordinating cybersecurity standards, policies, and procedures with federal agencies, coalition partners, and industry.

In this unclassified setting, I can state that as a matter of DOD enterprise cybersecurity, antivirus software does play a role. However, Kaspersky Lab is not part—a part of the Department of Defense antivirus solution. Currently, the DOD has enterprise licenses for both McAfee and Symantec Antivirus for DOD devices, as well as for DOD personnel's home computer use. Kaspersky Lab is not on the approved products list for the Department, and there are currently no contract awards for the software listed in the federal procurement data system.

Although the Department of Homeland Security's binding operational directive does not apply statutorily to defined national security systems, nor to certain systems operated by the Department of Defense, the Department has implemented the intent of the directive. Prior to the directive's release on August 3, 2017, Joint Force Headquarters DODIN Defense Information Network issued a task order to mitigate any potential threats to the Department networks. Within the bounds of the directive requirements, we conducted a search of DOD systems and confirmed that we did not have the listed Kaspersky products on any of our systems.

Kaspersky Lab products remain an ongoing supply chain risk management for the Department. To reduce these risks, DOD issued instruction 5200.44, protection of mission-critical functions to achieve trusted systems and networks. Additional details on that instruction are contained in my written statement, along with the detailed processes and enterprise resources DOD has implemented.

I would like to thank the subcommittee for supporting these important cybersecurity issues. Protecting the networks for the warfighter is a top priority for the Department of Defense. Thank you again for the opportunity to testify before you today, and I look forward to answering your questions.

[The prepared statement of Ms. Miller follows:]

STATEMENT BY

MS. ESSYE B. MILLER

DEPARTMENT OF DEFENSE (DOD)

DEPUTY CHIEF INFORMATION OFFICER (CIO) FOR CYBERSECURITY

BEFORE THE

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY OVERSIGHT SUBCOMMITTEE

ON

"Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive"

NOVEMBER 14, 2017

Introduction

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee today on the Department's position regarding the Federal government's use of Kaspersky Lab (KL) software.

I am Essye B. Miller, a member of the Senior Executive Service. I currently serve as the Deputy Chief Information Officer (CIO) for Cybersecurity at the Department of Defense (DoD). Additionally, I serve as the Department's Chief Information Security Officer (CISO). My primary responsibility is to ensure that the Department maintains a well-defined and executed cybersecurity program. I am responsible for coordinating cybersecurity standards, policies and procedures with federal agencies, coalition partners and industry.

As the Assistant Secretary of Defense for Legislative Affairs stated in his letter to the full Committee in September, the Department agrees with the assessment that trustworthiness and integrity of information technology performing cybersecurity functions is an important matter.

In an unclassified setting, I can reiterate that as a matter of DoD enterprise cybersecurity, antivirus software (AV) does play a role. However, KL is not part of the DoD's antivirus solution. DoD has enterprise licenses for McAfee and Symantec antivirus, for both DoD devices and for DoD personnel home computer use. Kaspersky Lab Antivirus software (KL AV) is not on the DoD approved products list, nor do we have any contract awards listed for this software in our Federal Procurement Data System.

Although the Department of Homeland Security (DHS) Binding Operational Directive (BOD) 17-01 "Removal of Kaspersky-Branded Products" does not apply to statutorily defined "National Security Systems" nor to certain systems operated by the DoD, the Department has implemented the intent of the Directive. Prior to the BOD's release, on August 3, 2017, Joint Force Headquarters-DoD Information Network (JFHQ-DODIN) issued Task Order 17-0207 KASPERSKY ACTIVITY to mitigate threats to the DODIN potentially posed by adversaries leveraging KL products installed on DODIN infrastructure. Within the bounds of the BOD's requirements, we conducted a search of DoD's systems and confirmed that we did not have the listed Kaspersky products on any of our systems.

While KL does not present the sort of problem for DoD that it may for other components of the Federal government, it remains an ongoing supply chain risk management (SCRM) problem. If the DoD operates untrusted hardware or software, whether performing cybersecurity functions or not, within its systems or networks, there is the risk that those systems and networks can be compromised.

In order to reduce these risks, DoD issued DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)" (November 12, 2012). The instruction outlines a multi-discipline approach to supply chain risk management, integrating systems engineering, SCRM, security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, assured services, and information systems security engineering. The policy, which applies to national security systems (NSS), establishes the DoD policy to identify mission critical functions and components, use all source intelligence analysis of the suppliers of critical components to inform risk management decisions, and apply risk management practices throughout the lifecycle, beginning in the design phase through the sustainment and operations phases.

To implement these policies in the Department, DoD has established and implemented the following processes and enterprise resources:

- A criticality analysis process, which identifies a system's mission capabilities, mission-critical functions, and system components associated with those functions, and allocates criticality levels to those components. This process allows a program to focus attention and resources on the system's most critical functions and components.

- A SCRM Threat Analysis Center (TAC) in the Defense Intelligence Agency (DIA) to provide supply chain threat assessments to programs on critical components.

- The Joint Federated Assurance Center (JFAC) to manage sharing of hardware and software (HW/SW) assurance testing capabilities and foster improved HW/SW test research and development. The JFAC Steering Committee is made up of representatives from the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), DoD CIO, the Military Departments, Defense Information Systems Agency (DISA), National Security Agency (NSA), Missile Defense Agency (MDA), National Reconnaissance Office (NRO), Defense Microelectronics Activity, and the Department of Energy.

- A Trusted Systems and Networks (TSN) Roundtable, which meets quarterly with Service and Agency SCRM Focal Points and other stakeholders and supports DoD-wide implementation of DoDI 5200.44, by sharing SCRM/TSN best practices and defining TSN-enterprise capability requirements. For example, the TSN Roundtable developed a TSN Mitigations Playbook to share best practices on how to mitigate a wide variety of supply chain threats and vulnerabilities. The TSN Roundtable has also shared best practices on criticality analysis process as it applies to the networks/information systems environment and prioritization of Requests for Information from the SCRM TAC.

To assist the interagency, DoD has also worked through the Committee on National Security Systems (CNSS), to issue the CNSS Directive 505, "Supply Chain Risk Management," which was recently updated. The Directive responds to challenges associated with SCRM and provides requirements for the U.S. Government to implement and sustain SCRM capabilities for NSS. This Directive (CNSSD No. 505) provides guidance for organizations while providing a "whole of government approach," resulting in enhanced inter-agency collaboration and the sharing of lessons learned to address SCRM.

DoD also co-chairs with DHS, the National Institute for Standards and Technology (NIST), and General Services Administration (GSA) the Software and Supply Chain Assurance Forum, a public-private forum bringing together industry-academia-government software assurance and supply chain risk management experts on a quarterly basis to share industry developments and best practices.

Conclusion

DoD recognizes the importance of the trustworthiness and integrity of information technology performing cybersecurity functions. The Department appreciates the support of the Subcommittee on these important matters and I would be happy to provide additional classified details on this issue in the appropriate setting. Thank you for the opportunity to testify today and I look forward to your questions.

CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF DEFENSE

Search Chief Information Officer

HOME ABOUT DOD CIO IN THE NEWS LIBRARY CONTACT US

Essye B. Miller
Deputy CIO for Cyber Security

DOWNLOAD HI-RES

Ms. Essye Miller, a member of the Senior Executive Service, is the Deputy Chief Information Officer(DCIO) for Cybersecurity, Department of Defense. In this position she acts as the department's Chief Information Security Officer (CISO). Ms. Miller is responsible for ensuring the DoD CIO has a well-defined and well-executed cybersecurity program. She is responsible for coordinating cybersecurity standards, policies, and procedures with other federal agencies, coalition partners, and industry.

Prior to joining the DoD CIO, Ms. Miller was the Director of Cybersecurity for the Army Chief Information Officer (CIO)/G-6. She was also the Army's Senior Information Assurance Officer and therefore was responsible for the development, implementation, execution, and oversight of the Army's Cybersecurity Program.

From November 2010 until August 2014, Ms. Miller served as the Director of Information Management and the Headquarters Air Force Chief Information Officer, Office of the Administrative Assistant to the Secretary of the Air Force in Washington, D.C. Ms. Miller also chaired the Architecture Configuration Control Board as part of the Pentagon Area CIO Council.

Previous to 2010, Ms. Miller served in various leadership positions throughout the Air Force, including the Air Force Communication and Information Center, Air Force Office of Warfighting Integration and Chief Information Office at the Pentagon, Air Combat Command at Langley Air Force Base, and the 75th Communications and Information Directorate and Deputy Chief Information Officer at Hill Air Force Base in Ogden, UT.

Ms. Miller earned her Bachelor of Arts degree from Talladega College, a Master of Business Administration Degree from Troy State University, and a Master of Strategic Studies from Air University at the Air War College. Additionally, Ms. Miller is Acquisition Level III certified in Information Technology.

She is a member of Armed Forces Communications and Electronics Association (AFCEA).

Chairman LAHOOD. Thank you, Ms. Miller.

At this time, I will recognize Dr. Jacobson for five minutes for his testimony.

TESTIMONY OF DR. MARK JACOBSON, ASSOCIATE TEACHING PROFESSOR, EDMUND WALSH SCHOOL OF FOREIGN SERVICE, GEORGETOWN UNIVERSITY

Dr. JACOBSON. Thank you. Mr. Chairman, Ranking Members, thank you for the opportunity and the kind introduction. I'm going to enjoy speaking with you all today. I hope I'm not too professorial for the hearing.

I also want to note that I'm here in my personal capacity and not representing any of my employers, the Navy Reserve, or the Department of Defense.

My intent is to try and put the Kaspersky situation within a larger foreign policy context. The Committee is already well aware of the dangers in the cyber arena and the imperative of cyber hygiene as a defense. I believe it's also critical to understand that Russian activities are part of broader foreign policy objectives, part of their political warfare campaign. Thus, regardless of whether or not there's a relationship between Kaspersky Labs and the Russian Government or it's simply a vulnerable piece of software, that becomes an entry point for Russian subversive activities, propaganda operations, or espionage.

Put simply, while cyber attacks and political warfare campaigns are a danger on their own, cyber activities that enable political warfare campaigns can prove incredibly effective at influencing attitudes and changing behaviors. Put another way, in political warfare campaigns, it is the human mind that is the center of gravity.

It's worth noting our adversaries have not hidden their intentions. Both the Russians and the Chinese have made it clear that they believe in the power of political warfare. Russia's well-financed and deliberate intervention in the American political dialogue is part of a broader effort to undermine America's faith in its free institutions, diminish U.S. political cohesion, weaken transatlantic relations, diminish the international appeal of the United States, and ultimately reduce American power abroad. Thus, we must think about U.S. national security more broadly rather than focusing on a single hack, one election cycle, or a single social media or antivirus company.

Propaganda and political warfare campaigns are certainly not new. It's worth noting that 500 years ago, Martin Luther's 95 Theses were probably the first element of intellectual thought to go viral. Of course, the Twitter of his day was the printing press and his own social media networks that allowed a message of religious reform to go viral and spread across all of Christendom in about four weeks. Today, that timeline might be four hours.

The Cold War also provides some insights into how the Russians think about disinformation and subversion. Soviet efforts not only included campaigns to discredit Martin Luther King and try and make the civil rights movement more extreme and more violent, but they also sought to provoke a full-blown race war in the United States. Perhaps more dramatically in 1983, the Soviets planted

newspaper articles alleging that the AIDS virus had been developed by the U.S. Government to target African Americans and the homosexual community. Within four years, that story had been repeated in over 80 countries, doing tremendous damage to U.S. credibility abroad and at home. Indeed, at least one study as late as 2005 found that almost 50 percent of African Americans believed HIV was a manmade virus designed to wipe out the African-American community.

Today, the fingerprints of Russian disinformation campaigns have been left on both sides of the Atlantic, whether it's Brexit or the American election, Russia propaganda still infects U.S. social media networks, and we see the same sort of divisive propaganda that we saw during the Cold War. Again, the goal is to divide and exploit divisions, yes, that already exist in our country, but they are exacerbating the problem.

So what do we do about this? While robust cybersecurity practices in the regulation of political advertising on social media are a good start, we must strengthen the public's ability to interact with information in the digital world. Broadly, we must begin a concerted effort to inoculate the American public against the viral threat of disinformation through more civic education and media literacy. Specifically, these must become bedrocks of our formal and informal education systems in order to make our population more immune to the threat.

This may require the same level of effort that President Eisenhower showed with the National Defense Education Act in 1958 in an attempt to bolster poor American efforts in math, science, and foreign language education. Indeed, Eisenhower believed those skills were critical in keeping up with the Russians during the post-Sputnik world. Today, it may be critical thinking and media literacy that can protect our freedoms.

To conclude, in 1900 Mark Twain celebrated the anniversary of the Gutenberg printing press, and he noted that everything that is good in the world today and everything that is bad is a result of that invention. That device had, in Twain's words, "found truth walking and given it a pair of wings, but it also found falsehood trotting and gave it two pair of wings. It had set peoples free but at the same time made despotism more possible where it was not possible before."

In short, the internet revolution may surpass Gutenberg's printing press is the greatest event in secular history, and it's already created wonderful opportunities and wicked problems. But we must understand that in the end it's used by human beings, and it's in human beings where we will need to strengthen, as the Chairman said earlier, resiliency.

Thank you very much, and I look forward to your questions.

[The prepared statement of Dr. Jacobson follows:]

Statement for the Record of
Dr. Mark R. Jacobson
Associate Teaching Professor
Edmund A. Walsh School of Foreign Service
Georgetown University

Before the
U.S. House of Representatives Committee on Science, Space, and Technology,
Subcommittee on Oversight
Hearing entitled:
"Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive"

November 14, 2017

Mr. Chairman, Ranking Member Beyer and distinguished members of the subcommittee. My name is Mark Jacobson, and I'm currently an Associate Teaching Professor at Georgetown University where I teach a number of courses in the Walsh School of Foreign Service. I've previously held several appointments at the Department of Defense and served as the first Deputy NATO Senior Civilian Representative in Afghanistan back in 2010-11. I'm also a former professional staff member at the U.S. Senate Committee on Armed Services. In addition to my civilian experience, I have had over twenty-three years as a reservist – in both the U.S. Army and U.S. Navy – and have mobilized twice on active duty, including to Afghanistan in 2006. I am also co-Author of a report entitled, *Shatter the House of Mirrors: A Conference Report on Russian Influence Operations*, and almost twenty years ago I was one of the first to address the problem of how the United States might respond pre-emptively or militarily to 'non-armed' subversive actions including cyber-attacks in an article entitled, *War in the Information Age: International Law, Self-Defense, and the Problem of 'Non-Armed' Attacks.* This challenge I note, remains with us today.

Thank you for the opportunity to appear before you to testify. I also wish to note that I am here today in my personal capacity and not representing any of my employers nor am I here as a member of the Navy Reserve or the Department of Defense.

My intent today is to try to help put the longstanding concerns that the U.S. government has had with Kaspersky Lab software into the larger foreign policy context. Cyber is, of course, but one arena for political, military, or economic action, albeit an incredibly powerful one. This committee is well aware of the dangers in the cyber-arena and the importance of strong cyber strategies, policies, and defenses in both the private and public sector. It is also difficult to overstate the imperative of "cyber hygiene." Without strong individual and group habits with regards to encryption, multi-factor authentication, password management, and the identification of phishing and similar online elicitation efforts, no cyber-security system will be effective.

In order, however, to fully understand the threats posed by viruses, back doors, or the type of front-door access that anti-virus companies like Kaspersky have, it is important to understand the overall objectives of the actors. In the case of nation-states, the nature of

their cyber activities is just a starting point as they are actions crafted to advance broader national foreign policy objectives. As you all know well, sometimes a cyber attack is simply an act of vandalism – to deface, annoy, or make an ideological point. Other times attacks are akin to more serious crimes such as robbery, blackmail, or the theft of intellectual property. Likewise, espionage is often the reason for cyber-intrusions into U.S. government and defense industry systems. I think we do a decent job of understanding these dynamics and activities – even if we cannot always totally prevent them.

What are of equal and sometimes greater worry for me are intrusions that are designed, in the end, to allow an actor to influence our attitudes and behaviors. Some intrusions may be designed to manipulate data. This is one of my greatest fears, especially considering the impact corrupt data that is believed to be accurate can have in the commercial, economic, and national security arenas. In short, manipulating data impacts our ability to understand what it is the data tells us, and not only can change our attitudes and perceptions but ultimately change our behaviors – perhaps leading us to make poor or even catastrophic decisions based on faulty raw data. Now imagine if manipulating data was part of an overall effort to influence our attitudes, perceptions, and behaviors. Imagine if data manipulation or obfuscation was coupled with public statements and news stories that supported that false narrative.

If there is but one thing to take away from my testimony today let it be that while cyber attacks and political warfare campaigns are a danger on their own, cyber-activities as part of an overall political warfare campaign are a particularly challenging threat, as they can prove incredibly effective at influencing attitudes and changing behaviors. Put another way, in political warfare campaigns and propaganda battles, it is the human mind that is the center of gravity.

It is worth noting that our adversaries have not hidden their intentions. For almost twenty-five years the Chinese have published the works of their military theorists in which the use of information warfare – which they believe will control the future of war – plays a central role in destroying an adversary's will and ability to fight. Similarly, in a doctrine that bears his name, the Russian Chief of the General Staff, General Valery Gerasimov, described that it was not effective for the Russians to match U.S. technological might, but rather to take an asymmetric approach and use a variety of information based tools, including the "use of technologies for influencing state structure and the population with the help of information networks."[1] These doctrines represent the digital equivalent of the age-old practice of political warfare and propaganda – efforts to create attitude and behavior change in a target audience. While cyber vulnerabilities can

[1] For a translation of the Gerasimov article describing his doctrine, see Robert Coalson's translation at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian- non-linear-war/

also lead to attacks on infrastructure, the larger strategic vulnerabilities are in terms of the pathways it provides to wage influence campaigns targeting elected leaders, opinion-makers, or the population at large in the U.S. and other democracies.

Thus, my bottom line is that we need to consider that attempts to infiltrate U.S. government systems are part of broader efforts to advance the Russian foreign policy agenda. In other words, it's not just about the "hack" but also about what is being done to the data. Is an adversary copying the data to use it later as ammunition in a classic disinformation campaign, or is the data being corrupted so as to create a false impression? Indeed, might there be times where we even decide not to let them know they have been discovered?

As Dr. Jim Ludes, and I noted earlier this year in a co-authored report, *Shatter the House of Mirrors,* we must consider that Russia's well-financed and deliberate intervention in American political dialogue is part of a much broader effort to undermine America's faith in its free institutions and diminish U.S. political cohesion; erode confidence in western democracies and the credibility of western institutions; weaken trans-Atlantic relationships, including NATO; diminish the international appeal of the United States as well as reduce American power abroad.[2] In other words, we have to get beyond 2016 and think about U.S. national security more broadly rather than focusing on a single hack, one election cycle, or a single social media or anti-virus company.

As in any war, the Kremlin's objectives are political. The principal weapon in this conflict is information, and the evidence of Russia's use of it in Europe and the United States is clear. With the advent of ever-expanding and precise communications technologies capable of manipulating public opinion at the individual level on a massive scale – in particular social media - the tools and tactics of influence developed over the course of the 20th century can alter perceptions of reality to a degree that they can shape societies, influence election outcomes, and undermine states and alliances. Regardless of whether there is a relationship between Kapersky Labs and the Russian government or the software was simply vulnerable to a state-actor, that software becomes an entry point for espionage, propaganda operations, or subversion. Thus in defending against non-armed assaults in the information age, we must not forget to focus on the intentions and objectives of the political actor – whether the Russians, Chinese, or a range of terrorist or criminal networks.

"What's Past Is Prologue"

The good news – propaganda and political warfare campaigns are not new. They are as old as the Bible and there are a variety of ways in which we can combat it and mitigate the consequences. It is worth noting that just over 500 years ago Martin Luther's "95 Theses" were promoted through the Twitter of his day. In this case the printing press combined with a variety of social networks allowed his message of religious reform to go "viral." As his friend Freidrich Myconius would note, "hardly 14 days had passed when

---

[2] James M. Ludes, PhD and Mark R. Jacobson, PhD, *Shatter the House of Mirrors: A Conference Report on Russian Influence Operations,* Salve Regina University, Pell Center for International Relations

these propositions were known throughout Germany and within four weeks almost all of Christendom was familiar with them."[3]Today, of course, those timelines might read 14 minutes and four hours.

The history of the Cold War provides us with an even better guide to how the Russians might use what was termed "active measures," or, political subversion, sabotage and information operations, including disinformation.[4] For the United States, these measures short of war, known as "political warfare" and encompassing both overt and covert operations were the most effective means to pressure the Soviet Union without risking a general conflict. For the United States, the emphasis was on engagement with the Soviet people and a strategy of exposing the truth and rot of the Soviet system in the hopes that the system would collapse from within. The Soviets also sought to expose flaws in the American system, notably the racial divide; but Moscow also sought to manufacture and spread deliberate disinformation about America. Going even further, these propaganda efforts were supported by subversive activities such as the Teacher's Riots in Japan in 1960 and an attack on Vice President Richard Nixon's convoy in Venezuela in 1958.

Even more dramatic efforts came in 1983, when Soviet intelligence operatives spread a "fake news" story with a pro-Soviet Indian newspaper alleging that the AIDS virus was developed by the U.S. government to target African-Americans and the homosexual community. Within four years the story had been repeated in the Soviet Union and in outlets in over 80 countries and in 30 languages.[5] The story did tremendous damage to U.S. credibility abroad as well as at home. At least one study as late as 2005 found that almost 50 percent of African-Americans believed that HIV was a "man-made virus" designed to wipe out the African-American community.[6]

As noted in our report, this was not the first Russian effort to stoke racial tensions and efforts to do so reached the heart of the Civil Rights movement:

> At the height of the civil rights movement, Soviet intelligence first sought to discredit Martin Luther King Jr. because he preached racial reconciliation. The Soviets favored instead more militant African-American activists who might provoke a full-blown race war in the United States. Towards that end, the Soviets generated a propaganda campaign to depict King as a collaborator with white oppressors. After his assassination, however, Soviet propaganda

---

[3] Margrethe Vestager, "Luther and the Modern World" Speech to the 9th Luther Conference, Copenhagen, 2016. Available at: https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/luther-and-modern-world_en

[4] The following paragraphs are adapted from Ludes and Jacobson, *Shatter the House of Mirrors.*

[5] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," INSS Strategic Perspectives No. 11, June 2012.http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf

[6] Darryl Fears, "Study: Many Blacks Cite AIDS Conspiracy," *Washington Post*, January 25, 2005, http://www.washingtonpost.com/wp-dyn/articles/A33695-2005Jan24.html?tid=a_inl

targeting the African-American community portrayed King as a martyr and sought to enflame the passions of the community already rioting in American cities.[7]

This was prologue for much of what we have seen in recent months and what we can expect to see in the future – divisive propaganda designed to exploit divisions in our country over race, guns, and LGBTQ rights – anything where they can drive those with different views to extremes. Clearly the Russians did not create the issues that cause division in the United States, but they are exploiting them and exacerbating the problems. Russia will overtly and covertly support organizations seeking secession or seeking to politically divide the United States and they will covertly press protest movements to move towards the extreme and ultimately violence, just as they did during the Cold War.

With so much of American political dialogue taking place over social media and with 67% of Americans receiving at least some of their news over social media it is not surprising that this platform has become a target for its Russian agents as well as their bots and trolls in an effort to create trends and increase the popularity of false narratives. The fingerprints of Russian government sponsored disinformation campaigns have been left on the Russian parliamentary election of 2011 and during the Scottish independence referendum of 2014, and there is some evidence of a Russian hand during the debate over "Brexit." I suspect we will see echoes of Russian involvement in the Catalonian independence movement and as seen in recent hearings on Capitol Hill. Russian social media propaganda still infects Twitter, Facebook and other U.S. based social media outlets and only now are we beginning to understand Chinese influence operations via these same platforms.[8]

So What Do We Do?

So what do we do about this? As I noted earlier in my testimony, in these battles to influence and persuade it is the human mind that is the center of gravity. We must think about how to strengthen the public's ability to interact with the information that it sees in a digital world.

In particular, we need to play to our strengths as a nation and perhaps our greatest strength is our belief in the free-exchange of information and the freedom of expression. Even when we disagree vehemently it is dialogue and discussion that will help bring transparency when actors seek to opacity. This may mean changes to the norms and potentially the regulations that govern social media. While we must respect the business model of the social media platforms, the social media companies must do more to combat

---

[7] Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield,* (New York: Perseus Books, 1999), 237-238.

[8] Mark Jacobson, "Target America: Dissecting Moscow's Social Media Campaign," *The Cipher Brief, October 31, 2017.* https://www.thecipherbrief.com/target-america-dissecting-moscows-social-media-campaign. On Chinese propaganda efforts see, "China Spreads Propaganda to U.S. on Facebook, a Platform It Bans at Home," *The New York Times,* November 8, 2017, available at https://www.nytimes.com/2017/11/08/technology/china-facebook.html

hate speech and weed out extremism as well as accept that they are as much "media" as they are "social." Accordingly, political advertisements on these platforms should face the same regulation they do in the print and broadcast arenas.

There may be need for changes in the traditional news arena as well. Even the most professional news organizations can be taken in by fabricated stories; the traditional news media may need to consider whether their current professional standards and practices allow them to identify when they have become a vehicle for a propaganda campaign.

Most importantly, we, as a nation must begin a concerted effort to properly educate the American public about the disinformation campaigns they face in the world today. It is critical we inoculate against the viral threat of disinformation through more education and training in the art of media literacy. Children and adults alike must be able to differentiate between advertisements and news articles and learn how to identify the source of information they find on the Internet. This will require significant efforts at the K-12 level in order to help students avoid falling prey to "fake news." While disheartening, it is important to note the findings of the Stanford History Education Group in recent reporting. Not only is it easy to "dupe" middle school, high school, and college students online, but also "experts" often fell victim to "easily manipulated features of websites, such as official-looking logos and domain names."[9] The silver lining in this report, however, was that trained fact-checkers did much better at correctly identifying legitimate sources and evaluating information. If we give our students and public the tools, they can do a great deal on their own to address this challenge.

Finally, the ability to evaluate information, think critically, maintain a healthy skepticism, and understand that some messages out there are deliberately deceptive will make our population much more conscious about the information they absorb. Likewise, it is the cornerstone of civic literacy – something that is sorely lacking in our toolboxes today. These educational imperatives are not easy tasks and it may require the same level of effort as seen with President Eisenhower's National Defense Education Act of 1958 – an attempt to bolster poor American efforts in terms of math, science, and foreign language education. Just as Eisenhower believed those skills were critical to keep pace with the national security threats in the post-Sputnik era; media, civic, and historic literacy alongside critical thinking may be what is needed to protect our freedoms today.

At the risk of sounding too professorial, I think it is important to conclude by reminding the committee of two letters that Mark Twain sent to celebrate the opening of the Gutenberg Museum in 1900. In them Twain reminded the world that Gutenberg's printing press was "incomparably the mightiest event" in history but brought with it not only a "new and wonderful earth" but a "new hell." Twain eloquently recounted the details, developments, and marvels that the new form of communication brought:

> It found Truth walking, and gave it a pair of wings; it found Falsehood trotting, and gave it two pair. It found Science hiding in corners and hunted; it has given it the freedom of

[9] Chronicle of Higher Education, *Teaching Newsletter: One Way to Fight Fake News,* November 9, 2017.

> the land, the seas, and the skies, and made it the world's welcome quest. It found the arts and occupations few, it multiplies them every year…It has set people's free, and other peoples it has enslaved; it is the father and protector of human liberty, and has made despotisms possible where they were not possible before.[10]

In short, Twain wrote, "what the world is today, good and bad, it owes to Gutenberg."

The Internet revolution may surpass Gutenberg's printing press as the "greatest event" in secular history – and yes, has already created new and wonderful opportunities and a plethora of wicked challenges. It may be used for good and for bad. In the end, however, it is used by human beings. The human dynamic, human intentions, and human solutions must remain at the forefront of our understanding of the problems and policy solutions.

---

[10] Mark Twain, Letter to the *Hartford Daily Courant*, June 27, 1900 and letter to the *Gutenberg-fest-zu-Mainz im jahre 1900*, 1901. Available at: http://www.twainquotes.com/Gutenberg.html

November 2017

Mark R. Jacobson

Dr. Mark Jacobson has over twenty years of experience in the U.S. government, international organizations, and academia working on some of the most complex and politically sensitive national security issues facing the United States. He has served as a policymaker, diplomat and academic in addition to being a combat veteran. He is a recognized expert on U.S. foreign policy and national security and can explain in clear terms how the U.S. develops foreign and defense policy, the role of Congress in these decisions, and how it all plays out in the international arena. He is currently an Associate Teaching Professor at Georgetown University's Edmund A. Walsh School of Foreign Service as well as a non-resident Senior Fellow at Salve Regina University's Pell Center for International Relations and Public Policy and a Senior Policy Advisor in the Government Affairs and Strategic Counsel Group at Kasowitz Benson Torres LLP.

Previously Jacobson held appointments as a Senior Advisor to the Secretary of Defense and Special Assistant to the Secretary of the Navy. Previously he served in Kabul, Afghanistan as the Deputy NATO Representative and Director of International Affairs at the International Security Assistance Force (ISAF) and in these roles advised Generals David Petraeus and Stanley McChrystal on the international political dynamics of the mission. Earlier in his career Jacobson served at the Pentagon in multiple roles and was in his office on September 11, 2001 when American Airlines Flight 77 crashed into the wing where he worked. On Capitol Hill, Jacobson worked for Senator Carl Levin on the staff of the Senate Armed Services Committee where he participated in the inquiry into the treatment and interrogation of detainees in U.S. custody. A combat veteran, his military service includes time as both an Army and Navy reservist including mobilizations to Bosnia in 1996 and to Afghanistan in 2006. As an academic Jacobson focuses on military history, the use of propaganda, as well as the politics of U.S. national security policy. He is currently drafting two books, one on the use of propaganda during the Korean War and the other on perceptions of the Carter Presidency, 1977-1981.

Jacobson grew up in the suburbs of Detroit, Michigan and holds degrees from the University of Michigan, the King's College, University of London and a PhD in Military History from The Ohio State University. He is a life member of the Council on Foreign Relations and a Senior Advisor to the Truman National Security Project. He lives with his wife and son in Washington DC and remains a rabid Michigan Wolverines fan.

Chairman LAHOOD. Thank you, Dr. Jacobson. And we will now move to the question portion of our hearing today.

And let me just thank all the witnesses for your valuable testimony here today for this important hearing. And the Chair now will recognize himself for five minutes.

And, Ms. Manfra, I want to start with you. It's my understanding that DHS notified Kaspersky of the BOD or the Directive 17–01 outlining the concerns that led to the issuance of the directive and provided Kaspersky the opportunity to initiate a review by DHS by providing a written response by November 3 of 2017. Did DHS receive a response from Kaspersky by that date?

Ms. MANFRA. Sir, we did give them a one-week extension to November 10, and we did receive a response.

Chairman LAHOOD. And have you initiated a review of that response?

Ms. MANFRA. Yes, sir. My legal counsel is reviewing the response right now.

Chairman LAHOOD. And can you give us an update on that today?

Ms. MANFRA. I cannot, sir.

Chairman LAHOOD. Can you tell us whether you've received any evidence or information from Kaspersky that addresses or alleviates the Department's concerns at this time?

Ms. MANFRA. I cannot say that we have. The legal counsel is still reviewing it. We just received it on Friday night. So once they review it, I will review it as well, and we'll make the determination to send it out to the Acting Secretary in order for her to make a decision.

Chairman LAHOOD. And have you reviewed it yourself?

Ms. MANFRA. Not yet, sir.

Chairman LAHOOD. Do you know how long it was, the response?

Ms. MANFRA. It was significant, sir. I'm not sure how many pages it was.

Chairman LAHOOD. And you referenced earlier your concern about litigation as it pertains to Kaspersky. Can you elaborate on that on your specific concerns?

Ms. MANFRA. Sir, the company, should we make a decision that they do not believe is appropriate, they always have the option to take this to court to have a judge make a decision about whether the Department made an appropriate decision.

Chairman LAHOOD. And have you reviewed the legal aspects of this, and have you made a determination on what was done here was legally proper?

Ms. MANFRA. I am not a lawyer, sir. I have had the lawyers review it and spoke with them about it. I do believe that it was legally proper.

Chairman LAHOOD. Ms. Manfra, the directive was issued on September 13, and within 30 calendar days, federal departments and agencies were required to identify the user presence of Kaspersky products on their systems and provide DHS a report containing preliminary findings such as the number of endpoints impacted by each product and the methodologies used to detect the presence of Kaspersky. Has DHS received this information from all agencies?

Ms. MANFRA. We have received it from the majority, sir. There are a small number of very small agencies that we are assisting them. They do not have the tools that other larger agencies might have, but we've received them from 94 percent of the federal agencies.

Chairman LAHOOD. And can you give us an update on what you have received thus far?

Ms. MANFRA. What we've received is that, again, out of all the federal agencies, a very small number have identified the use or presence in some aspect of their system of Kaspersky-branded products, about 15 percent of agencies who have reported.

Chairman LAHOOD. And where are you in the process of determining in the next phase whether anything was compromised or where we're at with that?

Ms. MANFRA. We're working with each agency individually. Some of them have chosen to go ahead and remove the products ahead of schedule, and so we're working to understand where the presence was, what doing an audit if you will of what information may have transited those systems and whether there was any cause for concern for the most part. We have not identified any yet, but we're still working with agencies.

Chairman LAHOOD. And do you believe the phased system that's been put in place, that you'll be able to comply with that fully?

Ms. MANFRA. Yes, sir.

Chairman LAHOOD. Within 60 calendar days of the issuance of the directive, agencies were required to develop and provide DHS a detailed action plan to remove and discontinue future uses of Kaspersky products. Since the 60-day deadline has passed, can you confirm that all agencies or departments have submitted their required action plan?

Ms. MANFRA. Not all of the agencies have submitted the required action plan. As I mentioned, some of them have gone ahead and just identified a way to remove the software, so they're going about that. A couple of the agencies needed additional help, so we're working with them on that so they can meet the deadline.

Chairman LAHOOD. Thank you. Those are all my questions at this time. I'll yield to Mr. Beyer for his questions.

Mr. BEYER. Thank you, Mr. Chairman. Thanks all of you very much for being with us. This is fascinating.

Dr. Jacobson, in your testimony—I'm going to quote from your written one because I have it written down. You said, "Russia's well-financed and deliberate intervention in the American political dialogue is part of a much broader effort to undermine America's faith in its free institutions, diminish U.S. political cohesion, erode confidence in Western democracies and the credibility of Western institutions, weaken transatlantic relationships, including NATO, and diminish the international appeal of the United States, as well as reduce American power abroad." I'd just love it if you could emphasize that this is a bipartisan concern, much larger than the 2016 presidential election.

Dr. JACOBSON. Thank you, Ranking Member Beyer. I grew up as a child of the Cold War and watched how Ronald Reagan strengthened U.S. efforts against the Soviets, but I also think it's interesting—and at the risk of invoking ire even from my Democratic

friends—so did Jimmy Carter in different ways. And I think that we had a bipartisan consensus throughout the Cold War that the Russians were a threat.

I actually—in listening to the Committee today, I see a recognition of that, and I think there's an understanding that there are things that need to be done to strengthen America's ability to be a strong ally abroad and look out for our vital national security interests that don't have to cross partisan lines. And I think if we look at what the Russian effort is doing and look at dealing with the technical, as well as dealing with this war against our population in terms of disinformation, I think there are a number of avenues where Congress can lead the way in terms of a bipartisan effort.

Mr. BEYER. Let me go further on that. I love the—Ph.D. in military history. It was a fascinating educational background. So as a professor, you talked about the human mind is the center of gravity in political warfare and then cited President Eisenhower with the whole notion of the ability to evaluate information, thank critically, maintain a healthy skepticism, understand the some messages out there are deliberately deceptive will make our population much more conscious about the information they absorb. How do we get there?

Dr. JACOBSON. It's a great challenge, sir. The Stanford History Education Group just did a study that's a bit disheartening, and what it did was take undergraduate students, high school students, as well as trained historians—my colleagues in the academic arena—and all of them failed pretty miserably at identifying fake news. The folks who did do pretty well were professional fact-checkers, and the reason is not only do they look for the source of information, they were comparing things horizontally. As I say to my students, "Watch MSNBC, watch CNN, watch Fox, even read Breitbart." You need to understand what everyone is doing about looking at a story, and you can pick up the anomalies. You can see what does not make sense.

But I think what's even more critical is to understand we have to start this at the K-through-12 level. By the time our children are 18 years of age, it's almost hardwired in their system where they can't identify or can't see the difference between an advertisement and a factual news article, an opinion piece, and false information. So this is an education issue. It's also a training issue as well, even for folks like myself, even for all of us sitting here today.

Mr. BEYER. Thank you. I confess the number of emails I get every week from family members that have the wildest possible theories, including the fact that Chairman LaHood and I are going to be paid our full salary for the rest of our lives after serving one day in Congress, that kind of disinformation is out there.

You talk about cyber hygiene imperative. You know, our electoral system is widely, widely distributed, you know, precincts. Virginia's got 2,500 precincts. How do we ever get cyber hygiene down to the towns and the counties around America?

Dr. JACOBSON. Again, I think the first step is awareness, but I'm actually glad I'm on this side of the table here and don't have to worry too much about implementation, but I think it's important to understand that this is not just a federal government issue; it's

a state and local issue as well. And the reason I emphasize cyber hygiene is all the technology in the world, as we used to say in the Army, is not going to G.I.-proof that computer against someone who picks up a USB stick on the sidewalk and decides to plug it into their computer. There are stupid things that smart people do that can help infect systems. And I think helping to make things easy for our federal workforce to understand in terms of what to do and what not to do but also educating the general public in terms of understanding malicious links.

And anyone who's looked at emails or read in the newspapers about even our most senior military leaders were duped by phishing attempts, this is difficult, but again, I think the solution in terms of teaching people what to do and what not to do is a bit easier than we might concede.

Mr. BEYER. Great. Thank you very much. Mr. Chair, I yield back.

Chairman LAHOOD. Thank you, Mr. Beyer.

I now recognize the gentleman from Florida, Mr. Posey, for his questions.

Mr. POSEY. Thank you, Mr. Chairman.

Ms. Manfra, it staggers the imagination that our government approved and purchased security software from Russia's Kaspersky Labs, known to have ties to the Kremlin's intelligence community. I mean, it's just—it's still hard for me to get my arms around the fact that we really allowed that to happen and that in fact that that software doesn't protect us. Obviously, it harms America's security by allowing malicious actors to get total access to our computers. Who approved the purchase of that software?

Ms. MANFRA. Sir, it's hard to say in every case. Often, what we see is that that software was bundled into other purchases, so you buy a computer and the antivirus was installed with the computer, so they weren't necessarily aware that they were explicitly purchasing that, which is why it took a little bit of time to—for agencies to go through and identify that. You know, in the end it is the procurement of individuals who are making some of these choices, but what we did see is a very low percentage of that presence. But for the most case, what we believe happened was it was often bundled into other purchases.

Mr. POSEY. So where does the buck stop?

Ms. MANFRA. Sir, in the end it is up to every agency head to make cybersecurity risk management decisions, and we are working across the federal government to approve—to improve our processes for supply chain risk management to be able to address issues such as this and to be able to make it clear what software and hardware agencies are purchasing and what risk that introduces into the system.

Mr. POSEY. Okay. So every agency head ultimately is responsible?

Ms. MANFRA. Yes, sir.

Mr. POSEY. According to the directives, already you were supposed to receive some reports from every agency that was affected. I think the Chairman asked you about that earlier. Would you mind stating for me which agencies have complied thus far?

Ms. MANFRA. Sir, all of the agencies have complied with the first phase except for a very small number of very small agencies who

just don't have the resources and we're helping them with that. We're still in the—sort of the second phase.

Mr. POSEY. When we say all the agencies except a few, how many agencies are we talking about?

Ms. MANFRA. Six, sir.

Mr. POSEY. Six agencies have complied?

Ms. MANFRA. Six have not complied yet with the first phase, which is the reporting whether they have the products on their system.

Mr. POSEY. How many have complied?

Ms. MANFRA. About—so, there's 102 total agencies, six—

Mr. POSEY. All right, 96, 98, okay.

Ms. MANFRA. Yes.

Mr. POSEY. Which agencies have not complied?

Ms. MANFRA. Sir, I'd be happy to work with your staff, not an open hearing, to talk to you about the specific agencies. They are working very hard, sir. It's not like they're—

Mr. POSEY. Well, I know they're——

Ms. MANFRA. —not trying—

Mr. POSEY. —working hard. I don't see, you know, what risk there is in naming who hasn't complied. I'm just curious. I don't know if other members are, but I'm curious to know which ones haven't complied.

Ms. MANFRA. We would prefer to keep those not public, sir. We don't believe that it is helpful to name them publicly.

Mr. POSEY. How would that harm anything?

Ms. MANFRA. I think it could have two aspects, sir. It would, you know, alert anybody who was looking to use potentially the presence of that software on their systems if—should they have it. It would also harm the relationship that we have. A lot of our work depends on a trusted relationship with these agencies.

Mr. POSEY. And so if you told Congress that they weren't behaving appropriately, it might hurt your relationship?

Ms. MANFRA. Sir, I don't mean to imply that they're not behaving appropriately. What I imply is that these are very small agencies, some of them with only 6 to 10 people in them that do not currently have the resources, and we're just assisting them with identifying what products are on their system.

Mr. POSEY. Now, you talked about fear of litigation from Kaspersky Labs a little while ago when somebody else mentioned that. How in the world could you possibly fear any action by them? I mean, you wouldn't have signed an agreement with them that would allow them to sue you and you not defend yourself, would you?

Ms. MANFRA. I don't fear any action from them, sir, but they do—they could potentially take action, and I want to ensure that we are in a position to address any concerns that a judge may have.

Mr. POSEY. Yes. I think the audacity—I think to paraphrase Clint Eastwood, "Go ahead and make my day."

Ms. MANFRA. Yes, sir.

Mr. POSEY. Can you explain to me the penalties to the executive agencies if they don't comply?

Ms. MANFRA. We would work with the Office of Management and Budget to determine what the issue was. Sometimes the issue is they don't have the resources, and whether it is to identify the products or it is to replace them, so it may not be a stick that they need but actually additional resources, or if there was a stick required, then we would work with OMB to address that.

Mr. POSEY. Have there been any enforcement actions thus far?

Ms. MANFRA. No, sir. We have issued six binding operational directives, and in each case every agency that we've worked with has been willing and eager to comply with them. Some of them are challenged with resources, though.

Mr. POSEY. Thank you, Mr. Chairman. I see my time's expired.

Chairman LAHOOD. Thank you, Mr. Posey.

I now yield to the Ranking Member, Ms. Johnson.

Ms. JOHNSON. Thank you very much.

Dr. Jacobson, you referred to fake news generated by the Soviet Union during the Cold War and cite the disinformation campaign by Soviets that claimed that the U.S. Government developed the AIDS virus intentionally to target homosexuals and African Americans. You say these stories spread to 80 countries and were translated into 30 languages in just four years, a timeline which today could probably be as little as 4 hours or perhaps 4 minutes to circulate around the world. You said one of the reasons the Soviets generated this fake story was to heighten racial divisions in America.

Just last month, CNN reported that Russia had created a fake group called Black Fist and Russian trolls linked to this operation paid personal trainers in New York, Florida, and other States to run self-defense classes for African Americans. They were apparently attempting to sow animosity and tension along racial lines. But this group was created in January of 2017, 2 months after the 2016 U.S. presidential election.

Dr. Jacobson, do you believe that Russia's influence campaign against America is only tied to trying to manipulate our elections or do they have other wider interests in influencing American citizens?

Dr. JACOBSON. Thank you, Congressman—Congresswoman. I believe the Russians have long-term objectives. They are not simply concerned with one election cycle. This is a campaign designed to continue to divide the United States. And if you take a look at some of the sites you've mentioned, you had mentioned Black Fist. There was also the Blacktivist, a fake site. There was also one called Heart of Texas. And the whole idea is to take the divide we have—and the Russians don't want to see reconciliation. They don't want to see dialogue and debate. What they would like to see is both sides of an issue resort to violence in the end. And I'm overstating the simplicity of doing that, but that's their long-term effort because it requires us then to look inside and not look at what's happening around the world and thereby advance Russian foreign policy objectives.

Ms. JOHNSON. You mentioned the need for better standards and fact-checking by reputable news organizations to help them avoid being duped by fake news. Social media sites are not newspapers, but they do generate news. At the same time, we don't want to

limit anyone's ability to speak out publicly and share their own thoughts or opinions, so how do we emphasize fact-checking in news-related stories and distinguish that from someone being able to offer their own opinion?

Dr. JACOBSON. I think there are a couple pieces there. I'll be the last person who wants to mess with the business model or content on social media sites. I mean, you look at one of the strengths of our nation, it's the idea of freedom of expression.

But I think there are certain limits we can place. For the social media world, they're are as much media companies today as they are social, and they have to understand that when it comes to political advertisements they should be subject to the same regulations that traditional media are.

I think there are ways—you look at a company like Twitter where there's a verification blue check that says to the world, "This individual is who they say they are." I also think if you look at systems like Moody's for the financial network, let's find an independent organization that gives a rating to either traditional or social media outlets. Now, not all the traditional or social media outlets will be particularly happy with it, but it's just a start. And in fact I'm—I believe that Silicon Valley could come up with some even better ways to do it if they put their mind to it.

Ms. JOHNSON. Thank you very much.

Mr. Chairman, I yield back.

Chairman LAHOOD. Thank you, Ms. Johnson.

I now yield to the gentleman from Louisiana, Mr. Higgins, for his questions.

Mr. HIGGINS. Thank you, Mr. Chairman. At this time I ask unanimous consent to enter into the record the written testimony of cybersecurity expert Troy Newman of Cyber5.

Chairman LAHOOD. Without objection.

[The information appears in Appendix II]

Mr. HIGGINS. Ms. Wynn, Mr. Newman has advised myself and other Members of this Committee that a simple software uninstall can't guarantee that all components of the application are removed. He elaborated that the best, most secure software removal process for remediation of threat is first an immediate uninstall and then a scheduled complete hard drive replacement. Can you briefly elaborate for those of us that don't understand things of this nature why a simple software uninstall is insufficient and why complete hard drive replacement is the best solution?

Ms. WYNN. Thank you for your question. I would have to take that back to some serious experts in terms of hard drive management and truly erasing software and breadcrumbs and footprints associated with that software that get left behind on hard drives. What I can speak to is that NASA takes very seriously its cybersecurity responsibility, and when we find unauthorized or unapproved software, we work very quickly to remove that.

We also have lines of defense that if—that are sort of layered in terms of—so that if you don't do very well on your first pass there are other ways and other mitigations that we do to protect our network to try to contain any threats to our environment.

Mr. HIGGINS. So when members of this panel have referred to agencies that have attempted to comply with the directive by re-

moving Kaspersky software from their systems, would you concur that that doesn't mean that Kaspersky is actually gone from the system?

Ms. WYNN. I would say that cybersecurity is never a 100 percent deal and that what we have to—

Mr. HIGGINS. If the hard drive is removed, is it a 100 percent deal?

Ms. WYNN. Sir, I can't speak to a hypothetical computer. I think you'd have to take a look at how a computer might be, let's say, infected to decide whether the hard drive was one where you could reuse again or if you would just decide not to put that hard drive back into your computer.

Mr. HIGGINS. So that would require—that's an excellent answer, thank you, Madam. And that would require further evaluation of that particular system?

Ms. WYNN. You need to always monitor your network to make sure it's fully protected.

Mr. HIGGINS. Very well. Thank you for your answer.

Ms. Manfra, thank you for your service to your country. The Binding Operational Directive 17–01 in its initial statement calls for a 30-day period to identify the use of Kaspersky products and then a 60-day period to provide detailed plans to remove and discontinue the present and future use of the products and then a 90-day period to begin to implement the agency plans to discontinue use and remove the products from information systems. However, there's a clause stating in there—stating that unless directed otherwise by DHS based on new information at—by what measure, Madam, would DHS ever determine never mind, let's go ahead and keep this product on our systems? Why is that clause in there?

Ms. MANFRA. Sir, after extensive review of this process by our legal counsel, we felt that it was important to allow Kaspersky Labs and any other potentially affected entity a meaningful opportunity to respond to the decision that we had made.

Mr. HIGGINS. So that clause is inserted into the DHS DOD 17–01, the binding operational directive for United States Government agencies—that clause was inserted to protect Kaspersky——

Ms. MANFRA. No, sir.

Mr. HIGGINS. —as opposed to government agencies?

Ms. MANFRA. No, sir. That clause was inserted that should the Kaspersky or another commercial entity come back with new information that would result in the Acting Secretary reconsidering her decision, then we would issue new guidance based off of that new information.

Mr. HIGGINS. And what could that new guidance be other than to discontinue the process of removing Kaspersky products?

Ms. MANFRA. That would probably be it, sir, if that was the Acting Secretary's decision but it would have to be based off of new information that had previously not been understood or considered.

Mr. HIGGINS. Mr. Chairman, I have one brief question if you would allow.

Chairman LAHOOD. Yes, go ahead, Mr. Higgins.

Mr. HIGGINS. Regarding code, Ms. Manfra, it's my understanding that the directive does not apply to Kaspersky code embedded into products of other companies. Is that correct?

Ms. MANFRA. I wouldn't say that it doesn't apply to Kaspersky code because that would be—

Mr. HIGGINS. The directive applies to removal of the products——

Ms. MANFRA. Correct, sir.

Mr. HIGGINS. —but what about the code behind?

Ms. MANFRA. It—what we focused on was products that is clearly identified as Kaspersky. What we have not focused on in this directive that we are continuing to pursue is understanding how they may be embedded in other products that are not Kaspersky and working toward the process to address those.

Mr. HIGGINS. Thank you for your answer.

Mr. Chairman, my time is expired. I would just share that it's concerning—it's exactly what we're talking about, the entire series of Kaspersky-related hearings, concerns, and apparently known or reasonably suspected information security threat that the Kremlin has embedded itself in our federal systems, and may I submit that that should certainly include code.

I thank you for your indulgence, Mr. Chairman. I yield back.

Chairman LAHOOD. Thank you, Mr. Higgins.

I now recognize the gentleman from California, Mr. McNerney.

Mr. MCNERNEY. Well, I thank the Chairman and I thank the witnesses.

Dr. Jacobson, three prominent U.S. security agencies including the CIA and the NSA, concluded that the Russians had operations intended to influence the 2016 presidential election but declined to comment on whether that effort had been successful. Do you have an opinion if the Russian efforts were successful in influencing the 2016 elections?

Dr. JACOBSON. Well, I'm cognizant of not getting ahead of where the multiple congressional investigations are, and of course I'm as eager to see what the conclusions are there, and I'm eager to see the U.S. intelligence community speak more publicly about this. What I am very confident in saying is that there is clear evidence of attitude changes amongst the U.S. population as a—in response to the numerous social media efforts undertaken by the Russians and Russian agents. And I would point to in particular a study by the Oxford Computational Propaganda project, which noted changes in the way—in the attitudes of individuals commenting on the election on social media after spikes in Russian-bot activity. But I have not done that original research, so I'm reliant on what they have done. But to me, as someone who worked on psychological warfare operations in the Army for quite some time, there is clear evidence of an attitude change amongst the population.

Mr. MCNERNEY. Well, has the Russian effort in any way diminished as a result of the publicity around the 2016 election?

Dr. JACOBSON. I don't think it's diminished. I think maybe the target sets have changed, so in short, no.

Mr. MCNERNEY. Okay. In your testimony you state that social media companies must start to see themselves more as media companies because their ability to spread information and influence the public. What actions can we take in Congress to ensure that the social media companies assume that responsibility more seriously, especially regarding political ads?

Dr. JACOBSON. As Dr. Jim Ludes and I said earlier this year in our co-authored report, it's probably time that the social media companies have the same standards in terms of regulation of political advertising transparency that traditional media companies have. I actually think the larger problem—so you have one problem of advertising—paid advertising on the social media networks. The larger problem is the one of fake sites, and I think that the continued dialogue between Congress, which I don't think wants to regulate the social media companies any more than necessary, and the social media companies which don't want regulation should continue this dialogue because their—the social media companies' terms of service are very powerful weapon against these fake sites. And we've actually already seen Facebook and YouTube use their terms of service to eliminate these fake sites, including one that was targeting veterans in particular.

Mr. MCNERNEY. Thank you. Ms. Miller, last month Reuters reported that H.P. Enterprises allowed a Russian defense agency to review the source code of H.P. cybersecurity software ArcSight as a condition of gaining certification to sell the product in Russia's public sector. In the same article, Reuters reported that ArcSight serves as a cybersecurity nerve center for much of the U.S. military and that vulnerabilities discovered during the source code review could make the U.S. military more vulnerable to cyber attacks. Is the DOD using ArcSight software?

Ms. MILLER. Sir, we use ArcSight primarily in our intel community, but unfortunately, I can't speak to the details at present.

Mr. MCNERNEY. Is the DOD taking steps to secure its systems since learning about the ArcSight code review?

Ms. MILLER. I would have to take that as a question for the record, sir.

Mr. MCNERNEY. Thank you. Does the DOD use any other software that's subject to source review by a foreign government—source code review?

Ms. MILLER. Well, actually, we have processes in place, sir, to help us work through that process, yes, we do.

Mr. MCNERNEY. Okay. Ms. Wynn, does NASA use ArcSight cybersecurity software?

Ms. WYNN. I'm trying to think about that for a second. We're going through a process of significant change in terms of the tools in the layers of our cyber defense, and I actually can't remember if ArcSight is coming in or leaving our network, so I'll take for the record and get back to you.

Mr. MCNERNEY. Okay. Ms. Manfra, same question. Does DHS use ArcSight cybersecurity software?

Ms. MANFRA. Yes, sir. I'll get back to you. We're working through a process to address this change similar to the other agencies.

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

Chairman LAHOOD. Thank you. At this time I yield to the Chairman of the full committee, Mr. Smith, for his questions.

Chairman SMITH. Thank you, Mr. Chairman. Just a comment, I'm really surprised our witnesses didn't have a better answer for the gentleman from California. I hope you will be able to answer my questions. And let me direct first ones, Ms. Manfra, to you. Are

you aware of any breaches to our national security that have been facilitated by the Kaspersky products?

Ms. MANFRA. Sir, I can't discuss that in this forum.

Chairman SMITH. I don't understand your answer.

Ms. MANFRA. Sir, I prefer to have that discussion in a classified——

Chairman SMITH. No, you don't need to have that in a classified hearing. I'm not asking for any specifics. I'm just asking if there have been breaches. I'm not talking about who had their systems breached, when it occurred, or how it occurred, just whether breaches did occur.

Ms. MANFRA. Sir, we're still working through the process to identify——

Chairman SMITH. We've heard that phrase several times today, "working through the process." That is just not sufficient of an answer.

Ms. MANFRA. Sir, is not conclusive at this time.

Chairman SMITH. You don't know whether or not systems have been breached by Kaspersky Lab products yet?

Ms. MANFRA. We do not currently have evidence that—conclusive evidence that they have been breached. I want to do a thorough review to ensure that we have a full picture of——

Chairman SMITH. What about the NSA employee? You don't think that was considered a breach?

Ms. MANFRA. Sir, I would have to direct any questions on NSA to the NSA.

Chairman SMITH. But sure—are you aware of that episode?

Ms. MANFRA. Sir, we'd have to have that discussion with the NSA.

Chairman SMITH. I'm not—are you aware of the episode and do you consider it a breach?

Ms. MANFRA. I'm aware of the allegations of what has been publicly reported in the press and would have to discuss any further details with the NSA.

Chairman SMITH. Okay. Let me try a different question. How did the Russian software—some people would consider it spyware—get on the approved list by Department of Homeland Security?

Ms. MANFRA. Are you referring to the GSA——

Chairman SMITH. Yes.

Ms. MANFRA. —sir? Yes. As I mentioned, we need to modernize our supply chain risk management processes within the government. Currently, our processes within the civilian government are largely focused on lowest-cost if you will.

Chairman SMITH. The fact that it was a Russian firm operated by a Russian who had some perhaps association with the KGB and certainly the Department of Defense and Russia, that didn't raise any red flags to anyone?

Ms. MANFRA. Sir, I wasn't a part of the GSA decision-making process. What I can say is that when we had enough information to make this risk decision, we engaged the GSA, NASA, and others who had these governmentwide contracts to begin to execute a process to remove it.

Chairman SMITH. But wasn't that after we called it to your attention? Didn't anybody see any red flags before that?

Ms. MANFRA. Yes, sir. One of the things when I assumed the acting position that I'm now appointed to in January was to conduct a thorough review of our use of Kaspersky, the intelligence associated with it——

Chairman SMITH. Yes, that's——

Ms. MANFRA. —and initiate a plan to remove it.

Chairman SMITH. Yes, that's not what I'm asking. That's after the fact. I'm asking about several years ago when it was on the approved GSA list. Are you aware of any agency that might have raised any red flags or not?

Ms. MANFRA. The government has been aware of some increasing concerns about Kaspersky, and we did—not me personally but the agencies with that information did engage with other agencies that had——

Chairman SMITH. Okay.

Ms. MANFRA. —those procurement responsibilities.

Chairman SMITH. I have a question to DOD about that in a second, but one other question. Did the license agreement with Kaspersky allow penetration beyond the usual type of agreements you have with similar types of companies?

Ms. MANFRA. No.

Chairman SMITH. Okay. We have pretty good evidence that that's not the case, and we'll get back to you on that and have a further discussion.

Ms. Miller, let me address a couple questions to you. We're under the impression that in 2012 the Department of Defense made a decision not to use Kaspersky Lab products. Are you aware of that or is that even true?

Ms. MILLER. Sir, I'm not even sure that was true. However, we have used processes that I can't discuss at this point based on intel information——

Chairman SMITH. Right.

Ms. MILLER. —to decide not to use the product.

Chairman SMITH. Okay. When did you decide not to use the products?

Ms. MILLER. I don't know a date, sir.

Chairman SMITH. A year?

Ms. MILLER. I don't have a year. I think it's been a couple, but I would have to check.

Chairman SMITH. Okay. It might have been 2012. I think we might have the same information. And can you say why they decided not to use—why DOD decided not to use Kaspersky Lab products?

Ms. MILLER. I cannot discuss that in open forum, but it was based on intel information that we had.

Chairman SMITH. And security—are you aware of any security breaches that occurred at DOD as a result of Kaspersky products?

Ms. MILLER. I have no knowledge of any within DOD.

Chairman SMITH. Itself, okay. And in 2012 or however many years it was ago that DOD decided not to use Kaspersky Lab products—and you say you'll get back to us as to why they decided that; there had to be a good reason I assume—do you know if they notified any other agencies of their concerns?

Ms. MILLER. I'm not aware of any notification, sir.

Chairman SMITH. Okay. Can you double-check that for me? And that'll be an easy question to find out. If you can get back to us by this afternoon on those two questions that I asked you.

And then a couple questions, Ms. Manfra, I asked you if you can get back this afternoon as well. They're easy to answer. And if you have to talk to me directly, that's fine, but I would ask you not to take advantage of the cover of classified unless individual's names are involved or unless it's in regard to specifics. If it's very general, that shouldn't be classified.

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

Chairman LAHOOD. Thank you, Mr. Smith.

I now recognize the gentleman from Colorado, Mr. Perlmutter.

Mr. PERLMUTTER. Thank you, Mr. Chair.

So Mr. Higgins talked about the Kremlin has embedded itself in the structure of the United States. And in prior hearings we've had conversations about foreign intelligence risk, espionage, meddling in U.S. affairs by the Russians and by Mr. Putin himself. And in Danang just a few days ago when asked about Russia meddling in U.S. affairs, the President said, quote, "I asked him again about meddling. You can only ask so many times. He said he absolutely"—he, Putin—"absolutely did not meddle in our election. He did not do what they are saying he did. I really believe that when he tells me that. He means it. I think he's very insulted if you want to know the truth."

So, Mr. Jacobson, you know, we're here and it's a real issue, Kaspersky having embedded itself potentially for the benefit of the Kremlin and Russia in our software, in our Defense Department, in NASA, in Homeland Security, but let me ask you about Mr. Putin and about whether or not, given his background, the President should just take him at his word. What do you think about that?

Dr. JACOBSON. Well, Mr. Putin's an ex-KGB officer. I'm not sure I would take him at his word if he told me the sun were shining and I was standing outside and there were blue skies and the sun was shining down on me.

Mr. PERLMUTTER. You used the word psychological warfare earlier. Would Mr. Putin be familiar with that? Is that something he did as the head of the KGB?

Dr. JACOBSON. Mr. Putin would be intimately familiar with not only operations he may have been involved in but the entire history of Soviet disinformation and propaganda campaigns. I mean, this is something embedded in the nature of KGB officers and not just propaganda designed to influence and shape American foreign policy that might be truthful. We're talking about deliberate attempts to mislead and obfuscate, covert action, sabotage, subversion, what have you. I don't trust anything coming out the Russian Government.

Mr. PERLMUTTER. And I appreciate the Chairman and the Republican majority for having this hearing and looking at Kaspersky and how it may have corrupted some of our computer systems, but, you know, when I take a look at the connections that this Administration has to Russia, Michael Flynn, Jeff Sessions had some contacts, Carter Page, Roger Stone, Jared Kushner, Donald Trump Junior, Michael Cohen, J.D. Gordon, Paul Manafort, Mr. Gates,

Mr. Papadopoulos. I mean, that's where this investigation, not just—should not just be on Kaspersky, which is coming in through the back door through different kinds of software that may have tainted the system, but what about the front door which is at the White House? So are you familiar with these different connections that this Administration may have with Russia?

Dr. JACOBSON. Only insofar as what I read in the newspaper. And like everyone else, I'm eager to see what the various congressional investigations or the Special Counsel's Office comes up with on this.

Mr. PERLMUTTER. You answered a question that Ms. Johnson asked you about, well, what's the real purpose? What is it that we're worried about? Why are we worried about Kaspersky having corrupted some of our systems? Why are we worried about these gentlemen with connections to Russia and with the President saying he believes Mr. Putin? What's the worry here?

Dr. JACOBSON. I think there are a couple things here. As we've heard during this hearing, there are concerns about—and it's not a back door; it's a front door. You know, we've given Kaspersky access—if I'm putting antivirus software on my home computer, I'm giving that software company some access. It can be used for espionage. It can be used—I'm particularly worried about data manipulation as well. But again with respect to my area of expertise, I think once you start to get into a system, it becomes a vector for propaganda and influence. It allows you to discredit federal organizations if you want. It allows you to manipulate data and try and create poor policy decisions.

But it's also part of a broader effort. If we think of cyber—and again the alleged Kaspersky situation is just one battle in a larger war. You know, imagine if cyber attacks augment rhetorical propaganda attacks that seek to influence the American people's attitudes on Ukraine or Syria or U.S. involvement in the NATO alliance. You can see how the ability of the internet to penetrate, to get to every single individual, and the ability of the Russians to take advantage of the enormity of the marketing data created by Facebook so they can tailor propaganda messages to individuals, it's something—we've never seen anything on that scale.

Mr. PERLMUTTER. Thank you. And I yield back.

Chairman LAHOOD. Thank you. Next yield to the gentleman from South Carolina, Mr. Norman.

Mr. NORMAN. Thank you, Mr. Chairman.

You know, as we in Congress hear your testimony and look back over the facts and what you're discussing, you know, I looked at your bios. You've each got, if you combine it, over 100 years in this area, so you're experts in what you do. As—if we look back over the time frame, Kaspersky didn't come up just recently, did it? When did—Ms. Manfra, when did this—the idea of having a problem with the product come up?

Ms. MANFRA. When I first became engaged was around 2014——

Mr. NORMAN. Okay. So this President has been here for nine months, so it's prior to this President coming into office——

Ms. MANFRA. Yes, sir.

Mr. NORMAN. —the issue came up.

Ms. MANFRA. Yes, sir.

Mr. NORMAN. Now, you mentioned—Chairman Smith mentioned the ULA agreements. Are you familiar with those?

Ms. MANFRA. Yes, sir.

Mr. NORMAN. Walk me through the process for approving a ULA agreement.

Ms. MANFRA. It's somewhat dependent on the agency, but generically, when a company decides to procure a certain software, they would receive what the company would like that end user license agreement to look like. In some cases we can negotiate some differences. Generally, we don't, but that is again a generic sort of process, so each agency might have different implementation.

Mr. NORMAN. So how many sets of eyes would look on a—would read a ULA agreement?

Ms. MANFRA. Ideally, you would have a legal review—well, you would absolutely have a legal review. You would also have the procurement officials involved, and ideally, you would also have the mission owners, and then you would have those individuals that are responsible for authorizing that network to operate and whatever software goes on that——

Mr. NORMAN. So a lot of eyes go on it and detail people that know or experienced in reading them.

Ms. MANFRA. Yes, sir.

Mr. NORMAN. And you say—I think your testimony was there's no abnormality in the ULA agreements that were signed?

Ms. MANFRA. No, sir.

Mr. NORMAN. Okay. Is it normal to agree to binding arbitration and no trial by jury? Is it normal to give access to all data, microphones, and cameras? Is that part of—is that boilerplate language that each agency would agree to?

Ms. MANFRA. Sir, I can't comment on what each agency boilerplate language is, but access to much of your computer system is often required for antivirus systems and security software, which was one of the reasons that we looked to understand how that data will be used and ensure we have a trusted relationship with that provider.

Mr. NORMAN. Well, I guess my question is do you—is it to waive a trial by jury?

Ms. MANFRA. That, sir, I would have to get back to on as to whether that was common practice.

Mr. NORMAN. Well, we have testimony by Mr. Newman that was an abnormality, that that was agreed to by somebody, somewhere, some agency.

Ms. MANFRA. It seems unusual, sir.

Mr. NORMAN. Okay. If—and you don't know which agency—your testimony was this agreement was reviewed by experts in the field, by a lot of different agencies. Now, if that's not a routine clause, who would have put that in there?

Ms. MANFRA. Sir, I'd have to understand the details of what the testimony is that you're referring to, the expert testimony, and we can get back to you with details on what might be unusual that that gentleman is referring to.

Mr. NORMAN. Okay. If you could get that in writing——

Ms. MANFRA. Yes, sir.

Mr. NORMAN. —to all of the members—anybody here that would be interested in seeing it. I think all of us would.

Ms. MANFRA. Yes, sir.

Mr. NORMAN. The exact language that was agreed to, any abnormality that was not normal——

Ms. MANFRA. Yes, sir.

Mr. NORMAN. —if you could highlight that, and then give us names of the different—I'm sure there are lawyers within the agencies that would agree that looked at this—give us some names of who looked at this ULA agreement.

Ms. MANFRA. I will do my best, sir.

Mr. NORMAN. I yield back.

Chairman LAHOOD. Thank you. I now yield to Mr.—the gentleman from Georgia, Mr. Loudermilk.

Mr. LOUDERMILK. Well, Thank you, Mr. Chairman.

Ms. Wynn, in 2013 the Science Committee staff emailed the legislative affair teams at NASA to ensure that Kaspersky Lab was not being used on any NASA systems. Do you have any record of that request?

Ms. WYNN. No, sir, I'm not aware of that request, but I can certainly check on the record status within NASA. I didn't join NASA until 2015.

Mr. LOUDERMILK. Okay. If you would and get back to the Committee on that, I'd appreciate it.

Today, you testified that Kaspersky Lab products were identified on a small number of machines that had access to the NASA internal network. Is that correct?

Ms. WYNN. Yes, that's correct.

Mr. LOUDERMILK. Okay. What was the time frame that Kaspersky was present on the NASA systems? Was it after 2013?

Ms. WYNN. We discovered between 2013 and the assurances that we did in recent past that there had been Kaspersky on the network. Our belief is that it was part of either a larger procurement or bundled within a series of software that then, because our tools are getting smarter, able for us to identify it and go ahead and get that removed.

Mr. LOUDERMILK. Okay. So some of it may have been software bundled on a computer that was purchased?

Ms. WYNN. It could have been within a computer that was purchased or within a package of software that was put on the network.

Mr. LOUDERMILK. Can you tell us why it was not remedied earlier and disclosed to the Committee as part of the response to the Chairman's July 27 letter to all departments and agencies?

Ms. WYNN. So at NASA we've been working very hard to deploy the continuous diagnostic and mitigation tools which allow us to have absolute insights to every single part of NASA's IT infrastructure, which is over 160,000 components. Prior to the CDM coming on board, NASA's ability to take a look at its entire footprint was fragmented and therefore pulling together and synthesizing an entire picture was very, very difficult to do that.

Mr. LOUDERMILK. Okay. Ms. Manfra, on October 10 the New York Times reported additional details regarding hackers working for the Russian Government stealing details about the NSA's cyber

capabilities from a contractor who had stored the information on his home computer. I think everyone is aware of that report. These new revelations were that Israeli intelligence uncovered the breach and the Russian hackers' use of Kaspersky software. The article details that "Israeli intelligence officers informed NASA that in the course of their Kaspersky hack, they uncovered evidence that Russian Government hackers were using Kaspersky's access to aggressively scan for American Government classified program." This thing reads like a Clancy novel, spies spying on spies. But in your opinion would this be considered concrete evidence that Kaspersky Lab has ties to the Russian Government?

Ms. MANFRA. Sir, I can't make a judgment based off of a press reporting, but I understand the allegations outlined in that report, and should those be true, I would say that that was evidence, yes, sir.

Mr. LOUDERMILK. So if the intelligence community were to verify this, then you would agree that that's concrete evidence there's ties?

Ms. MANFRA. Yes.

Mr. LOUDERMILK. Okay. Thank you for your candor there. If this happened in 2014 and the NSA was alerted immediately, why did it take until 2017 for action to take place to secure our systems by removing the software?

Ms. MANFRA. Sir, the binding operational directive was just the latest in a series of actions that we have been taking within the government over the past few years to address this. We had been briefing at a classified level across the federal government, as well as critical infrastructure, as well as—as much unclassified information as we can share. I was not satisfied with the progress, and so we looked for other avenues to escalate to ensure that we had full removal across the federal government.

Mr. LOUDERMILK. But it took three years to really take action once this was known?

Ms. MANFRA. Sir, we—this is a more recent authority that we were given. It is just, again, one of the tools that we had. We were exhausting all of the tools through information-sharing mechanisms throughout, again, the government and others, and this was just one of the public tools that we took to remove the——

Mr. LOUDERMILK. Okay.

Ms. MANFRA. —software.

Mr. LOUDERMILK. Dr. Jacobson, in a recent interview with Reuters, Mr. Kaspersky admitted his company widely used antivirus software to copy files from personal computers, files that did not pose a threat to the personal computers of those customers. I worked 30 years in the IT business. I did not know this as being a standard practice. Is this typical of industry to copy files that are known not to be threats?

Dr. JACOBSON. Congressman, I don't know. I don't have that sort of expertise. However, what I will say is that I stopped using Kaspersky years ago just because of the first sets—this has to be maybe four, five years ago—because there were a number of articles in trade journals that suggested that they just didn't have the types of standards that you want if you're a home computer user so—but beyond that, I can't answer your question.

Mr. LOUDERMILK. Ms. Miller, is there any other antivirus software that you know that would copy files not known to be threats?

Ms. MILLER. None that I'm——

Mr. LOUDERMILK. Okay.

Ms. MILLER. None that I'm aware of, sir.

Mr. LOUDERMILK. All right. Thank you.

Ms. Manfra, last question. Would you review—would a review of Kaspersky's Lab source code, as recently offered by the CEO of Kaspersky, help alleviate concerns or is this merely a publicity stunt?

Ms. MANFRA. Sir, I have heard the offer to review the source code, and while we would welcome opportunity to hear from Kaspersky on what potential new information and mitigations they could put in place, the source code review would not be sufficient in my opinion.

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

Chairman LAHOOD. Thank you. I have a few additional questions here to ask.

Ms. Miller, you commented earlier that the Department of Defense at some point made a determination based on intelligence that you were not going to engage with Kaspersky products. Is that correct?

Ms. MILLER. Yes, sir, based on threat information and other intel feeds that we had.

Chairman LAHOOD. In that threat information and concerns, was that information relayed to DHS or other agencies?

Ms. MILLER. I'm not aware—not sure, sir. I would have to confirm.

Chairman LAHOOD. And do you know why that information wouldn't have be relayed? Are you saying it could have been relayed and you're not aware of it?

Ms. MILLER. It could have been relayed and I'm not aware of it. I would have to confirm.

Chairman LAHOOD. Okay. And how long will it take you to confirm that and get that back to the committee on that?

Ms. MILLER. We can do that within the next day or so, sir.

Chairman LAHOOD. Okay. Ms. Manfra, are you aware of the intelligence information that DOD relied upon when they made the decision not to engage with Kaspersky products?

Ms. MANFRA. I believe I'm aware of the same information, sir, yes.

Chairman LAHOOD. And when did you become aware or when did the Department become aware?

Ms. MANFRA. I would have to get back to you on when the Department became aware. I can tell you that I first became aware of concerns in the 2014 time frame.

Chairman LAHOOD. And can you tell us why a similar decision in 2014 wasn't made similar to what DOD did?

Ms. MANFRA. Some agencies such as the Department of Homeland Security did engage in an effort to remove the Kaspersky software from their systems. What we identified was largely agencies who are more security-focused or had the ability to receive classified briefings or removing the software. Where there was a gap was in the civilian agencies that did not have that infrastructure nec-

essarily in place where they could rely on classified information to make procurement decisions. So we wanted to provide further direction across the civilian government for them to be able to make the same choices based off of the risk management decisions that we had made.

Chairman LAHOOD. Ms. Manfra, does the September 2, 2017, directive apply to federal contractors?

Ms. MANFRA. Yes, sir.

Chairman LAHOOD. Okay. And to your—can you give us an update or where is it at? Have all federal contractors been compliant? Where is that at in terms of your follow-up with them and how do you keep track of that?

Ms. MANFRA. We have a couple of different mechanisms to keep track. Every agency is responsible for defining what contractors constitute their federal information system and reporting that up to us. What we see is what the agencies report to us. We also, as I mentioned, have sensors deployed both internal to agency networks as well as at the perimeter that can identify what agencies may be calling out to Kaspersky IP addresses so that that would indicate that they probably have it on their systems as well. So we're looking at a variety of different avenues to identify whether they have it. And that would include a contractor system if they identify it to us. However, it is up to the agency to identify that contractor system to us.

Chairman LAHOOD. And do you feel like you have full knowledge of all the contractors that the different agencies engaged with?

Ms. MANFRA. I do not—I could not say that I have full knowledge of all the contractors that agencies engage with. I can say that for all of the largest agencies I feel very confident that they have done an assessment of not only the internal government-owned and -operated networks as well—but as well as the contractor-owned or -operated networks and systems. But there—to say that I have full insight into every contractor that the civilian government uses, I probably do not have that right now.

Chairman LAHOOD. Ms. Miller, in previous testimony before this committee, cybersecurity experts stated, quote, "The Federal Government should take the lead on developing a trusted vendor list that provides guidance on approved cybersecurity vendors with a secure supply chain that agencies can have confidence in," unquote. In your opinion, how would the federal government go about establishing such a trusted vendor list? And what agencies should lead the federal government's effort to do so?

Ms. MILLER. Sir, I'll start with the second question. I'm not sure what agency I would recommend leading it, but I think we have a responsibility as we work with our vendors to ensure we have supply chain management processes in place to evaluate what they're bringing to us. We've established relationships with DIA and the—what—I can't think of the acronym right now—that give us an opportunity to identify critical components where supply chain managements are of real concern and put processes in place to help us avoid any risk introduced by our industry partners.

At the same time, we have had very strong conversations with members of the defense industrial base to make sure they understand risk associated with use of the Kaspersky products, and the

Defense Security Service has directed all of them to remove the products for any—especially of our classified systems. And we're working with our unclassified—or our vendors in the unclassified arena now with the Defense Federal Acquisition Regulation clause that we've put in place to help them not only understand the risk but to understand the products that they're using and their responsibility to protect government information and the government network as they relate to mission operations.

Chairman LAHOOD. Thank you. That's all my time.

Mr. Perlmutter, I recognize you for additional questions.

Mr. PERLMUTTER. Just a couple questions about Kaspersky, and this is to the whole panel.

In October 2015 the U.S. subsidiary of Kaspersky Lab, which is called Kaspersky Government Security Solutions, paid President Trump's former National Security Advisor Lieutenant General Michael Flynn $11,250 for a speaking fee. So just to the panel I would ask, are you aware of anybody from your agencies speaking at any Kaspersky conferences not for payment but just as one of their speakers? And what is it again, Dr. Jacobson, that we're worried about to have a guy like Michael Flynn speaking at a Kaspersky conference? Some open-ended questions, start with you, Ms. Manfra. Do you know if anybody from GSA or your agency has spoken at any Kaspersky conferences?

Ms. MANFRA. Sir, we not done a thorough review of speaking engagements at Kaspersky-sponsored events. I can say that we—the guidance to my workforce is to not engage with Kaspersky-sponsored events.

Mr. PERLMUTTER. Ms. Wynn?

Ms. WYNN. I am not aware of anyone speaking at a Kaspersky-sponsored conference, and I would say that there is a thorough vetting review by our Office of General Counsel with respect to any speaking engagements of NASA personnel.

Mr. PERLMUTTER. Ms. Miller?

Ms. MILLER. Sir, same with DOD. We go through a rigorous review with the general counsel before we approve speaking engagements, and to my knowledge, we've not had any DOD employees speak at a Kaspersky event.

Mr. PERLMUTTER. Dr. Jacobson?

Dr. JACOBSON. Can I provide you a very unsatisfying answer? You know, I don't know the specifics of that case, but I think this is exactly why we need to understand that the Russians are going to continue to try and find key influencers, whether in government or in the media space or amongst the public, to help them with their information or disinformation campaigns in the United States. I mean, all foreign governments try and influence the United States. That's why we have laws that regulate the level of transparency there.

But let me also state that this is why I think there's a great opportunity for a bipartisan sponsored commission like the 9/11-style commission, the Iraq study group, or the Afghanistan study group to really look forward and see how do we combat information campaigns or disinformation, whether it's Russian, Chinese, or terrorist networks in the future? And that would be a last point in terms of urging what the committee and Congress overall could do.

Mr. PERLMUTTER. Well, and to that point, again, sort of looking for these different crevices or potential vulnerable spots, in December 2016 Kaspersky Lab awarded $18,000 in funding to three universities to help identify and—to help develop identity and verification methodologies for secure online voting systems. So, you know, obviously, they're looking for different places to take advantage of, you know, America and an open—pretty open system that we have.

Just curious, if you were at DHS, Ms. Manfra, if you were advising these universities, what would you advise them about speaking and taking money from Kaspersky Lab? It's a very hypothetical question and it calls for speculation on your part, but I'm still going to ask it.

Ms. MANFRA. Yes, sir. I can't presume to advise a university on what money they might take or engagements they might speak at, but I would encourage them to ensure that they consider the risk associated with those interactions as a part of their engagement and their funding.

Mr. PERLMUTTER. Dr. Jacobson?

Dr. JACOBSON. Well, I'm definitely not speaking for Georgetown University here, but I was thinking of three things. If I was asked today whether I would advise a university on that, I would think about three things: one, politically, it would be absolutely unacceptable to do given what's going on with Kaspersky and the allegations in the committee right now; second, from a public relations perspective, it would be a really bad idea; and third, there's prudence. We know in the university and think tank world there's certain countries and certain companies you just really think twice about taking money from, and again, if someone asked me, I would recommend they not take it today.

Mr. PERLMUTTER. Okay. I yield back.

Chairman LAHOOD. Thank you, Mr. Perlmutter.

That concludes our questions today. I would just advise that the Committee—the Oversight Subcommittee on this is going to continue to monitor this situation, and as the directive continues to get implemented, we look forward to continuing to work with you on this issue. It's important that we as a committee and subcommittee stay engaged on this, and we'll look forward to the next phase of our hearing series on this and look forward to continuing to work with you.

With that, our hearing is concluded. Thank you.

[Whereupon, at 11:53 a.m., the Subcommittee was adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Ms. Jeanette Manfra

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"

Ms. Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications,
Department of Homeland Security

Questions Submitted by Ranking Member Donald S. Beyer, Jr.,
Subcommittee on Oversight,
House Committee on Science, Space, and Technology

Question 1: During the hearing, in response to questions about federal government computers using Kaspersky Lab software, you stated that of the federal government computers found using Kaspersky Lab software, most were not specifically procured by the respective agencies, but came from bulk hardware purchases with Kaspersky Lab software pre-installed.

Does your agency ever accept pre-installed software on agency-purchased computers?

Response 1: Yes

Question 1A: If so, please indicate the security process the agency uses to minimize the security threat these acquired computers can pose?

Response 1A: Computers are occasionally purchased with a standard software suite, as specified in purchase orders and license agreements. Computers that are purchased for small deployments (e.g., pilots) are manually hardened and patched, and all unapproved software (as defined by the Technical Reference Manual (TRM)) is removed and replaced with approved products. This process is monitored and overseen by the applicable Information System Security Manager (ISSM) and Information System Security Officer (ISSO) for the information system.

Question 1B: Does the agency have a policy of "wiping" all purchased computers before connecting them to the agency's computer network?

Response 1B: Computers that are purchased in bulk are routinely wiped before connection to the network, with the existing pre-installed software replaced with a standardized, DHS-created image that has been appropriately patched and hardened against computer threats. This image consists only of software that is approved for deployment in the Department, based on the Technical Reference Manual (TRM).

Question 2: According to information on its website, Kaspersky Lab offers software development kits for integration into third party hardware and software. Some Kaspersky Lab products are reportedly used within other companies' hardware products, including

those of Cisco, Juniper and Microsoft-though these relationships are not always explicitly disclosed in product information.

What efforts has your agency taken to insure that Kaspersky Lab software embedded in third-party products is eliminated from federal government systems, as ordered by DHS Binding Operational Directive (BOD) 17-01, issued on September 13, 2017?

Please indicate the number of Kaspersky Lab subcomponents identified in third party hardware or software on your agency's network, if any.

Response 2: Binding Operational Directive (BOD) 17-01, Removal of Kaspersky-Branded Products, requires agencies to take actions in regards to Kaspersky-branded products on federal information systems. The BOD does not address Kaspersky code embedded in the products of other companies.

Question 3: Have any of your agency's contractors or subcontractors indicated that they have searched for Kaspersky Lab subcomponents in third party hardware or software on computer products that are connected to your agency's networks?

Response 3: In light of ongoing litigation, the Department respectfully declines to provide new, non-public information related to Kaspersky Lab or BOD 17-01 at this time.

Question 4: Have any of your agency's contractors or subcontractors indicated that they have discovered Kaspersky Lab subcomponents in third party hardware or software on computer products that are connected to your agency's networks?

Response 4: In light of ongoing litigation, the Department respectfully declines to provide new, non-public information related to Kaspersky Lab or BOD 17-01 at this time.

Question 5: If so, please indicate how many Kaspersky Lab subcomponents they have identified and if they have all been removed.

Response 5: In light of ongoing litigation, the Department respectfully declines to provide new, non-public information related to Kaspersky Lab or BOD 17-01 at this time.

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"

Ms. Jeanette Manfra,
Assistant Secretary for Cybersecurity and Communications,
Department of Homeland Security

Questions Submitted by Representative Ralph Norman

Question 1: Does the September 12, 2017, directive apply to federal contractors?

Response 1: DHS is authorized to issue a Binding Operational Directives (BOD) for the purpose of safeguarding federal information and information systems from an information security threat, vulnerability, or risk. BOD 17-01, Removal of Kaspersky-Branded Products, applies to federal information systems. A "federal information system" is defined as an "information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency." This definition is drawn from Office of Management and Budget Circular No. A-130. Each department and agency is responsible for determining whether a given information system, including an information system used or operated by a contractor, meets this definition.

Question 2: On Oct. 27th, the DHS Federal Network Resilience chief Michael Duffy detailed that DHS is leaving a determination up to the individual agencies if and when to pass along the Kaspersky Lab products ban to the agencies' contractor, based on their own risk assessments.

Why did DHS tailor its directive to just federal civilian agencies? Why did it not include language guiding the agencies on how to deal with their contractors' use of Kaspersky products?

Is DHS confident that this plan will result in the quickly ending the use of Kaspersky products on federal systems, including federal contractors?

What if an agency makes a determination that based on their own risk assessment they will not pass the ban along to their contractors?

Does DHS see this as a blatant disregard of the purpose of the ban?

Response 2: DHS is authorized to issue a Binding Operational Directives (BOD) for the purpose of safeguarding federal information and information systems from an information security threat, vulnerability, or risk. BOD 17-01, Removal of Kaspersky-

Branded Products, applies to federal information systems. A "federal information system" is defined within the BOD as an "information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency." This definition is drawn from Office of Management and Budget Circular No. A-130.

BOD 17-01 requires that departments and agencies identify any use or presence of Kaspersky products on all "federal information systems" within 30 days. As agencies conducted this assessment, DHS advised agencies that contractors may need to be contacted, and the systems they operate assessed for the presence of Kaspersky-branded products. DHS has advised agencies that contracting officers and contracting officer representatives should work together to provide direction to their contractors, as appropriate.

Question 3: On September 28, 2017, DOD issued a memorandum directing all contractors in the National Industrial Security Program that use classified information systems to remove all Kaspersky software or hardware from their systems.

Are each federal department and agency required to issue a formal memorandum to its contractors that mandates cessation and removal of Kaspersky products from contractor-managed systems, like DOD did?

Response 3: No. DHS is authorized to issue a Binding Operational Directives (BOD) for the purpose of safeguarding federal information and information systems from an information security threat, vulnerability, or risk. Binding Operational Directive (BOD) 17-01, Removal of Kaspersky-Branded Products, applies to federal information systems. A "federal information system" is an "information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency." This definition is drawn from Office of Management and Budget Circular No. A-130.

BOD 17-01 requires that departments and agencies identify any use or presence of Kaspersky products on all "federal information systems" within 30 days. As agencies conducted this assessment, DHS advised agencies that contractors may need to be contacted, and the systems they operate assessed for the presence of Kaspersky-branded products. DHS has advised agencies that contracting officers and contracting officer representatives should work together to provide direction to their contractors, as appropriate.

Responses by Ms. Renee Wynn

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"

Ms. Renee Wynn, Chief Information Officer,
National Aeronautics and Space Administration

Questions Submitted by Ranking Member Donald S. Beyer, Jr., Subcommittee on Oversight, House Committee on Science, Space, and Technology

Question 1: **Pre-installed Software on Agency Computers**
During the hearing, in response to questions about federal government computers using Kaspersky Lab software. Ms. Manfra from the Department of Homeland Security stated that of the federal government computers found using Kaspersky Lab software, most were not specifically procured by the respective agencies, but came from bulk hardware purchases with Kaspersky Lab software pre-installed.

Question 1a:

Does your agency ever accept pre-installed software on agency-purchased computers?

Answer 1a:

All Enterprise-managed computers are wiped and the systems are reloaded with a NASA approved software load.

Question 1b:

If so, please indicate the security process the agency uses to minimize the security threat these acquired computers can pose?

Answer 1b:

N/A

Question 1c:

Does the agency have a policy of "wiping" all purchased computers before connecting them to the agency's computer network?

Answer 1c:

All Enterprise-managed systems are wiped and reloaded with a NASA approved software build prior to joining the NASA network as part of the contractor's standard operating procedure to deploy new seats. NASA's policy on desktop standards is currently being updated to formally document this requirement.

Question 2: **Kaspersky Lab Subcomponents on Federal Networks**
According to information on its website, Kaspersky Lab offers software development kits for integration into third party hardware and software. Some Kaspersky Lab products are reportedly used within other companies' hardware products, including those of Cisco, Juniper and Microsoft-though these relationships are not always explicitly disclosed in product information.

Question 2a:

What efforts has your agency taken to insure that Kaspersky Lab software embedded in third-party products is eliminated from federal government systems, as ordered by DHS Binding Operational Directive (BOD) 17-01, issued on September 13, 2017?

Answer 2a:

NASA uses a baseline software suite and core load for its devices to comply with Federal requirements for desktop computers, laptops, and other end user devices. If a system owner requests the installation of software not approved by NASA, the NASA Office of the Chief Information Officer (OCIO) must approve individual instances and accept a level of risk. The NASA CIO has not approved any installations of Kaspersky Lab Products.

To identify and mitigate installations of Kaspersky, whether embedded or not, NASA uses enhanced scanning tools as a part of the DHS Continuous Diagnostics and Mitigation (CDM) program. These tools scan all IT assets and monitor network traffic on systems connected to the Agency network. Manual scans and inquiries at the local level are also performed. As of the response to BOD 17-01 to DHS on October 13, 2017, NASA has identified no active installations of embedded or non-embedded Kaspersky Lab Products.

Additionally, the NASA Office of Procurement (OP) searched Agency and Federal procurement databases to determine if there are documented purchases of said software at NASA during the timeframe of your query. OP searched the Agency's System for Award Management (SAM), the Federal Procurement Data System – Next Generation (FPDS-NG) and records for the NASA Agency Purchase Card Program. OP also searched for records utilizing the NASA IT Security – Enterprise Data Warehouse (ITSEC-EDW) system. The OP found no record of Agency funds being used to purchase individual instances of Kaspersky Lab software.

Question 2b:

Please indicate the number of Kaspersky Lab subcomponents identified in third party hardware or software on your agency's network, if any.

Answer 2b:

As of October 13, 2017, NASA has identified no active instances of Kaspersky Lab

subcomponents in third party hardware or software on the Agency's network.

Kaspersky Lab software is not part of the Agency's enterprise-licensed, core-load anti-virus software. Since 2010, NASA has used Symantec Endpoint Protection as its core-load anti-virus solution under our End User Service contract.

Question 2c:

Have any of your agency's contractors or subcontractors indicated that they have searched for Kaspersky Lab subcomponents in third party hardware or software on computer products that are connected to your agency's networks?

Answer 2c:

NASA Security Operations Center (SOC) actively monitors the network for any potential Kaspersky Lab related communications and Agency contractors perform regular enterprise network and local scans to identify vulnerabilities as part of NASA's Continuous Monitoring Program. These scans include searching for Kaspersky Lab subcomponents in third party hardware and software connected to the Agency's networks.

Question 2d:

Have any of your agency's contractors or subcontractors indicated that they have discovered Kaspersky Lab subcomponents in third party hardware or software on computer products that are connected to your agency's networks? If so, please indicate how many Kaspersky Lab subcomponents they have identified and if they have all been removed.

Answer 2d:

NASA's process for discovering Kaspersky Lab subcomponents involves enterprise and local level scans for any connections to the NASA network, in combination with manual inquiries at the system owner level. All subcomponents in third party software or hardware connected to the Agency's networks have been identified and mitigated, as reported in BOD 17-01. As of Dec. 6, 2017, NASA OCIO is unaware of any indication from a contractor or subcontractor that they have discovered Kaspersky Lab subcomponents in third party hardware or software on computer products.

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"

Ms. Renee Wynn,
Chief Information Officer,
National Aeronautics and Space Administration

Additional Material from Representative Loudermilk,
Subcommittee on Oversight

In 2013 the Science Committee staff emailed the legislative affairs team at NASA to ensure that Kaspersky Lab was not being used on any NASA systems. Do you have any record of that request?

In November 2013, staff from the House Science and Technology Committee contacted NASA to inquire about whether NASA was using Kaspersky Lab (KL) software. Given the less-advanced network insight tools available to NASA at that time, NASA's Office of the Chief Information Officer conducted a quick• turn data call to Center CIOs and determined that no Center at that time had record of any use of KL products. At the same time, NASA's Office of Procurement searched its database and determined that there were no records of individual purchases of KL software. Since the 2013 inquiry, NASA's IT management and network insight tools have greatly improved, and thus NASA cybersecurity officials have been able to better identify and remove unauthorized software on NASA's network, including limited instances of KL software, as explained in Ms. Wynn's testimony. It is important to note that identification of and removal of any unauthorized software at NASA is an ongoing process, and it is not an action that was prompted specifically by the Department of Homeland Security's Binding Operational Directive 17-01.

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"

Ms. Renee Wynn,
Chief Information Officer,
National Aeronautics and Space Administration

Additional Material from Representative McNerney,
Subcommittee on Oversight

Does NASA use ArcSight cybersecurity software?

NASA does use the software as part of its multi-layered approach to cybersecurity protection efforts. However, we cannot provide more detail about the Agency's use of this software via non-secure communications channels.

Responses by Ms. Essye Miller

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"

Ms. Essye Miller,
Deputy Chief Information Officer for Cybersecurity,
Department of Defense (DOD)

Questions Submitted by Ranking Member Donald S. Beyer, Jr.,
Subcommittee on Oversight,
House Committee on Science, Space, and Technology

QFR#1): Pre-installed Software on Agency Computers

During the hearing, in response to questions about federal government computers using Kaspersky Lab software, Ms. Manfra from the Department of Homeland Security stated that of the federal government computers found using Kaspersky Lab software, most were not specifically procured by the respective agencies, but came from bulk hardware purchases with Kaspersky Lab software pre-installed.

QFR#1A) Does your agency ever accept pre-installed software on agency-purchased computers?

A #1A): In accordance with Deputy Secretary of Defense (DSD) memo, "Implementation of Microsoft Windows 10 Secure Host Baseline," February 26, 2016, all authorized general-purpose Windows workstations must be configured with the DoD Microsoft Windows 10 Secure Host Baseline as the operating system prior to connecting to a DoD network. The only authorized method for obtaining this baseline is via the Defense Information Systems Agency Information Assurance Support Environment portal. Access to the information on the portal is limited to authorized personnel who are authenticated by DoD Common Access Card (CAC). The process for a first-time installation of Microsoft Windows 10 Secure Host Baseline includes a "wipe and load" process that removes unauthorized, pre-installed software.

In February 2016, the DSD directed a Department-wide deployment and transition to a single operational baseline for all Windows computers in order to strengthen our cyber security posture. By March 31, 2018, the entire DoD is required to complete the transition to the Microsoft Windows 10 Secure Host Baseline. The DoD Microsoft Windows 10 Secure Host Baseline brings consistency to department host security configuration management activities. The Secure Host Baseline is a configuration unique to DoD and includes a list of required and optional software applications. This application list is based on existing DoD cyber security requirements. Changes to the list requires Authorizing Official approval.

QFR#1B) If so, please indicate the security process the agency uses to minimize the security threat these acquired computers can pose?

A QFR#1B): The DoD has policies and procedures that minimize these risks at various levels of the hardware life cycle. DoD Directive 8500.01E, Information Assurance, April 23, 2007, and DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology, define the policies and processes for accrediting new systems prior to deployment. They define comprehensive steps to identify vulnerabilities caused by non-compliant security controls (such as those found in unapproved, pre-installed software).

DoD has established and continuously updates a Security Technical Implementation Guide for Microsoft Windows 10 Secure Host Baseline. It provides a standard configuration that is applied for all general-purpose Windows computers across the Department. Any changes to the baseline configuration must be reviewed and authorized by the Designated Approving Authority (DAA) prior to connecting the workstation to a DoD network. These changes would include pre-installed software that is not approved for use on DoD computers.

QFR#1C) Does the agency have a policy of wiping all purchased computers before connecting them to the agency' computer network?

A QFR#1C) Per our response to QFR#1A, the process for a first-time installation of Microsoft Windows 10 Secure Host Baseline includes a "wipe and load" process that removes unauthorized, pre-installed software. Use of the Microsoft Windows 10 Secure Host Baseline was directed by the DSD.

QFR #2): Kaspersky Lab Subcomponents on Federal Networks

According to information on its website, Kaspersky Lab offers software development kits for integration into third party hardware and software. Some Kaspersky Lab products are reportedly used within other companies' hardware products, including those of Cisco, Juniper and Microsoft-though these relationships are not always explicitly disclosed in product information.

QFR #2A) What efforts has your agency taken to insure that Kaspersky Lab software embedded in third-party products is eliminated from federal government systems, as ordered by DHS Binding Operational Directive (BOD) 17-01, issued on September 13, 2017?

A#2A): BOD 17-1 explicitly excluded embedded software. "This directive does not address Kaspersky code embedded in the products of other companies." The BOD specifically noted that it does not apply to statutorily defined "National Security Systems" or to certain systems operated by the Department of Defense or the Intelligence Community. DoD has decided to pursue this course of action without external direction. USCYBERCOM issued OPORD 17-0182 followed by JFHQ-DoDIN FRAGORD 7 to TASKORD 17-0207.

Additionally, on September 28, 2017, the Defense Security Service (DSS) issued a Memorandum signed by National Industrial Security Program (NISP) Authorizing Official Karl Hellmann directing that effective immediately, all NISP contractor facilities possessing classified information systems under DSS cognizance and authorization are directed to remove all Kaspersky Labs software and/or hardware from the authorized information systems. DSS also

published the information on their external website and published the same information in the October 2017 "Voice of Industry."

QFR #2B) Please indicate the number of Kaspersky Lab subcomponents identified in third party hardware or software on your agency's network, if any.

A #2B): JFHQ-DODIN is currently gathering this information on subcomponents that include embedded Kaspersky Lab software on the Department's networks. **QFR #2C) Have any of your agency's contractors or subcontractors indicated that they have searched for Kaspersky Lab subcomponents in third party hardware or software on computer products that are connected to your agency's networks?**

A #2C): DoD has not requested, nor has it received unsolicited, this information from our contractors or subcontractors.

QFR #2D) Have any of your agency's contractors or subcontractors indicated that they have discovered Kaspersky Lab subcomponents in third party hardware or software on computer products that are connected to your agency's networks? If so, please indicate how many Kaspersky Lab subcomponents they have identified and if they have all been removed.

A #2D): DoD has not requested, nor has it received unsolicited, this information from our contractors or subcontractors.

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"

Ms. Essye Miller,
Deputy Chief Information Officer for Cybersecurity,
Department of Defense (DOD)

Questions Submitted by Representative Ralph Norman

QFR#1) Does the Directive apply to the Department of Defense?
a) If not, then why not?

A QFR#1) The BOD specifically noted that the it does not apply to statutorily defined "National Security Systems" or to certain systems operated by the Department of Defense or the Intelligence Community. In addition, DoD is statutorily exempted from Department of Homeland Security Binding Operational Directives by 44 U.S.C. 3553. The authority of the Secretary of Homeland Security granted in 44 U.S.C. 3553 (b) explicitly excludes national security systems (NSS) (per 44 U.S.C. 3553 (d)) and DoD information systems (per 44 U.S.C. 3553 (e)). DoD information system was defined as: "systems that are operated by DoD, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense."

While the BoD does not apply to NSS or DoD systems, the Department, after careful consideration of available information and consultation with interagency partners, took actions to properly protect its systems.

QFR#1B) It is my understanding that DoD has taken steps to carry out the intent of the Directive, Is that correct?
(i) If yes, can you briefly describe the steps DoD has taken to carry out the Directive's intent?

A QFR#1B): Prior to DHS Binding Operational Directive (BOD) 17-01's release, on August 3, 2017, Joint Force Headquarters-DoD Information Network (JFHQ-DODIN) issued Task Order 17-0207 KASPERSKY ACTIVITY to mitigate threats to the DODIN potentially posed by adversaries leveraging KL products installed on DODIN infrastructure. DoD conducted a search of its systems and confirmed that listed Kaspersky products were not on any DoD systems. DoD CIO reported this response to DHS.

QFR#1C) It is also my understanding that DoD DSS issued a memorandum to National Industrial Security Program (NISP) contractors ordering the identification and removal of Kaspersky installations. Is that correct?

(i): Why did DoD issue this memorandum and undertake this course of action? Was it for the purpose of ensuring consistency across the federal government, or was it based on DoD's specific concerns with respect to the use of Kaspersky products?

A QFR#1C): On September 28, 2017, DSS issued a Memorandum signed by NISP Authorizing Official Karl Hellmann directing that effective immediately, all NISP contractor facilities possessing classified information systems under DSS cognizance and authorization are directed to remove all Kaspersky Labs software and/or hardware from the authorized information systems. Additionally, DSS published the information on their external website and published the same information in the October 2017 "Voice Of Industry".

DSS issued the memorandum to be consistent across the federal government in response to the "DHS Statement on the Issuance of Binding Operational Directive 17-01" and comply with DoD intent and directions. Furthermore, DSS wanted to ensure that cleared defense contractors were aware of potential threats/risks to warfighter critical technologies and DoD classified information.

QFR# 2) Is there a concern that if one contractor is using Kaspersky Lab products, there is a possibility of a user being able to jump from system to system if there is a slight interaction? Wouldn't this put the supposed "cleared" federal systems at risk still from Kaspersky touched products?

A QFR#2): DoD is not aware of this capability at this time. The activity is not a characteristic of any anti-virus programs.

QFR#2a) Is there an effective way to monitor the traffic of a federal system to ensure this would not happen?

A QFR#2a): As a rule, the Department does not discuss in an unclassified setting the specifics of network operations in public.

Responses by Dr. Mark Jacobson

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Bolstering the Government's Cybersecurity:
A Survey of Compliance with the DHS Directive"

Dr. Mark Jacobson,
Associate Teaching Professor, Edmund Walsh School of Foreign Service,
Georgetown University

Question submitted by Representative Ralph Norman

1. Is there a concern that if one contractor is using Kaspersky Lab products, there is a possibility of a user being able to jump from system to system if there is a slight interaction? Wouldn't this put the supposed "cleared" federal systems at risk still from Kaspersky touched products?
    a. Is there an effective way to monitor the traffic of a federal system to ensure this would not happen?

1. Unfortunately, I do not have the technical background to answer this question or the sub-question, 1a. I believe my fellow panelists, however, may be able to answer these technical questions.

Appendix II

Additional Material for the Record

STATEMENT SUBMITTED BY MR. TROY NEWMAN, PRESIDENT, CYBER5

TROY A. NEWMAN

Troy Newman written testimony for the hearing November 14, 2017 before the Oversight Subcommittee of the Committee on Science, Space, and Technology.

Thank you for the opportunity to appear and provide testimony regarding DHS BOD 17-01. It is my duty as a citizen and a patriot to provide any knowledge and guidance based upon my experience in technology and cybersecurity.

The purpose of this hearing it to examine and assess the implementation of DHS BOD 17-01 by federal government departments and agencies **identifying** Kaspersky Lab Software on their systems, taking action to **remove** the software, and **reporting** to DHS.

We are faced with a significant risk having foreign based and governed security software running on our federal government computing assets. Furthermore, I believe this same threat goes beyond the federal government and reaches into the private business sector putting at risk the intellectual property of many businesses.

Foreign owned AV software is not the only cybersecurity threat we as a nation face. In recent months, we have discovered how social media has been utilized by foreign states to sway public opinion. We have witnessed IoT devices, mostly of foreign manufacture, falling victim to mal-ware from foreign nations and being staged to then form attacks on our infrastructure. Whether this situation is calculated and planned, or simply a result of the proliferation of all things digital, really does not matter. What does matter is we have legitimate threats inside our borders on a massive scale that must be mitigated. In cybersecurity terms, we must ensure the CIA triad; the Confidentiality, Integrity, and Availability of our information assets. I believe the Kaspersky issue, addressed by BOD 17-01, is the tip of the proverbial iceberg.

Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004

TROY A. NEWMAN

CISSP Certified Information Systems Security Professional

I am providing a high-level overview for this discussion. I am not privy to the current network configurations of each federal agency system or to the complete scale of Kaspersky Lab Software use in those systems.

To effectively implement DHS BOD 17-01 several actions must be taken in succession.

First the affected systems must be identified.

To identify the systems affected by current or previous use of Kaspersky Labs Software there must be an assessment of each department and agency network. Software tools, written by American software companies and governed by federal law, can facilitate this assessment process and produce reports of the findings. From the reports and asset lists, a remediation list can be generated. Based upon asset access to sensitive information a rapid impact analysis should be completed to prioritize system remediation and expedite the mitigation processes.

Assessment Requirements:

- Physical access to each agency network.
- Network diagram of each agency network.
- Network credentials to run full asset list software/hardware discovery.
- If the software was run on servers, it may be necessary to perform additional steps.
  - Access list and group membership reporting.

Next the software must be completely removed from the identified affected systems.

To determine the level of software removal required, we must consider the level of risk incurred with exposure of the system. In my opinion, leaving any component of the software resident on the system is an extremely high-risk exposure. A simple software uninstall, while a necessary first step, cannot guarantee that all components of the application are removed, especially when considering the depth of access granted this security application. The best, most secure, software removal process for remediation is first an immediate uninstall then a scheduled complete hard drive replacement. While hard drive replacement may sound expensive, this solution may actually be a more cost-effective approach than the additional highly involved uninstall and clean up procedures that would be necessary without hard drive replacement. The hard drive replacement process also provides additional security benefits such as upgrading and standardizing systems to a COE, common operating environment. For security purposes, no outdated systems should remain in use. Systems meeting minimum specifications can be remediated with hard drive replacement. Those not meeting minimum specs should be retired.

Secure software Removal Requirements:

- Access to assets for immediate uninstall – network access for programmatic uninstall of software via policy for systems participating in a Windows Domain and secure remote control as an alternate method.
- Determine if system meets minimum specifications (used for "remediate with hard drive replacement" or "replace entire asset" decision).
- Physical access to systems meeting minimum specs for scheduled hard drive replacement.

Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004

- Software list by duty function (there should be COE for each agency role).
- Software licensing and installation media.
- New COE hard drive installed *preconfigured* with applications & defense in depth software (OS Secured, Anti-Virus, Secure DNS).

- Physical access to systems for secure retirement of assets not meeting minimum specs.

Finally, reports on remediation efforts must be compiled and delivered to DHS.

To accurately report there should be a chain of command within each agency designated to submit the findings from the initial assessments and then to provide reports on the remediation. Ongoing network analysis and continuous monitoring is required to ensure there is no outbound or inbound traffic other than that expected/approved. Monitoring reports should be generated on a daily basis with automated alerts for anomalies sent for immediate review. This is handled with a managed security platform including firewall and DNS reporting through a security operations center. Going forward, quarterly reports should be delivered from each agency to a DHS oversight committee.

Reporting Requirements:
Communication directory.
Reporting standard.
Reporting repository.
Network monitoring tools.
Review of network monitoring and reporting protocol for anomalies (IRP – incident response plan).
SOC

TROY A. NEWMAN

CISSP Certified Information Systems Security Professional

A holistic approach should include the five disciplines of the NIST Cybersecurity Framework.

1. Identify - Assess -
   a. How many systems impacted?
   b. Where are the system physically located?
   c. Data classification to zone network segments.
2. Protect -
   a. Immediate removal of the software.
   b. Immediate traffic monitoring of networks (data ingress and egress).
   c. WISP review & training.
3. Detect -
   a. Continue monitoring network traffic at the perimeter firewalls.
   b. Continue monitoring network connections.
   c. Continue measurement of the network utilization (bandwidth by asset and by protocol).
   d. SIEM (Security Incident & Event Management) systems to facilitate threat detection.
4. Respond - Remediation -
   a. Verify software removal.
   b. Implement COE (common operating environment) based upon role.
   c. Replace HDD.
   d. Review network access, external connectivity, based upon role requirements.
   e. Incident response plan in place for network anomalies detected through monitoring systems.
5. Recover -
   a. Incident analysis to provide feedback and further improve security posture.
   b. Secure CIA of any potentially affected information

Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004

TROY A. NEWMAN

CISSP | Certified Information Systems Security Professional

Sample Assessment Report for Computers: Should be generated for all managed resources

- Computer Name
- IP Address
- Systems resources – CPU – RAM – HDD
- Health Status – AV, Disk, Security Logs, Services, Events
- Software list

Workstation Summary

	CPU	RAM	OS	HDD Usage	AntiVirus	Disk	Intrusion	Usability	Services	Updates	Events	Backup
E	1.90 GHz	3.9 GB	Win8 x64	28%								
Model: Microsoft Corporation Surface Pro 2												
Status: Standby/Hibernate for 00h 43m				IP: 192.168.1.115	100%	58%	100%	89%	1%	38%	41%	
31	3.70 GHz	15.9 GB	Win8 x64	69%								
Model: Dell Precision T3610												
Status: Standby/Hibernate for 00h -30m				IP: 192.168.1.67	100%	82%	100%	89%	1%	98%	24%	
002	3.70 GHz	15.9 GB	Win8 x64	74%								
Model: Dell Precision T3610												
Status: Running for 1d 12h 13m				IP: 192.168.1.112	100%	83%	100%	89%	1%	98%	48%	
003	3.70 GHz	15.9 GB	Win8 x64	44%								
Model: Dell Precision T3610												
Status: Running for 8d 23h 16m				IP: 192.168.1.113	100%	83%	100%	89%	1%	98%	18%	
	3.10 GHz	3.9 GB	Win7 x64	15%								
Model: Dell OptiPlex 3010												
Status: Running for 8d 23h 29m				IP: 192.168.1.110	75%	83%	100%	89%	1%	98%	100%	
E	2.60 GHz	7.9 GB	Win7 x64	37%								
Model: Dell Latitude E7450												
Status: Running for 09h 04m				IP: 192.168.1.75	100%	100%	100%	89%	1%	84%	47%	
CE	2.30 GHz	3.9 GB	Win7 x64	54%								
Model: Dell Latitude E6530 non-vPro												
Status: Disconnected for 13d 02h 26m				IP: 192.168.1.53	88%	100%	100%	100%	1%	87%	51%	
R	2.60 GHz	7.9 GB	Win7 x64	40%								
Model: Dell Latitude E7450												
Status: Running for 10h 27m				IP: 192.168.1.72	100%	100%	100%	89%	1%	93%	84%	
	3.10 GHz	3.9 GB	Win7 x64	45%								
Model: Dell OptiPlex 3010												
Status: Running for 1d 10h 54m				IP: 192.168.1.58	100%	100%	100%	89%	100%	98%	97%	
3	3.60 GHz	15.9 GB	Windows 1	16%								
Model: Dell OptiPlex 7050												
Status: Standby/Hibernate for 1d 22h 02m				IP: 192.168.1.54	100%	100%	100%	100%	1%	81%	84%	
J	2.60 GHz	7.9 GB	Win7 x64	38%								
Model: Dell Latitude E7450												
Status: Standby/Hibernate for 26d 08h 03m				IP: 192.168.1.51	100%	90%	100%	89%	1%	98%	43%	
	2.60 GHz	15.9 GB	Windows 1	35%								
Model: Dell Latitude E7470												
Status: Running for 8d 11h 38m				IP: 192.168.1.90	100%	100%	100%	89%	1%	98%	84%	
	3.10 GHz	8.0 GB	Win7 x64	43%								
Model: Dell OptiPlex 390												
Status: Running for 12d 23h 21m				IP: 192.168.1.59	100%	100%	100%	89%	1%	84%	87%	
A	2.60 GHz	15.9 GB	Windows 1	24%								
Model: Dell Latitude E7470												
Status: Running for 17d 16h 27m				IP: 192.168.1.85	100%	82%	100%	89%	1%	90%	100%	
h	2.60 GHz	7.9 GB	Win7 x64	34%								
Model: Dell Latitude E7450												
Status: Running for 1d 11h 08m				IP: 192.168.1.62	100%	100%	100%	89%	1%	98%	87%	

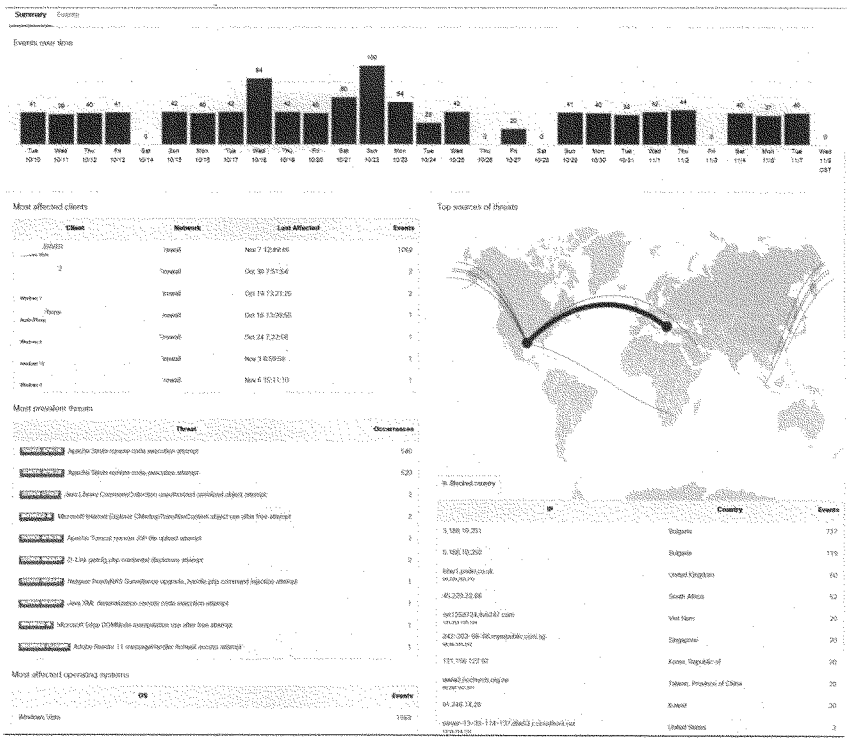
Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004

TROY A. NEWMAN

CISSP® Certified Information Systems Security Professional

Continuous network monitoring recommendations:
In order to further identify potential data breach, network traffic needs to be monitored and an incident response plan must be in place.

Sample Firewall Security Reports: Should be available for all managed resources.
Identify the threats origination, threat vector, number of attempts.
Provide a means of blocking traffic and IP addresses.



Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004

TROY A. NEWMAN

CISSP® | Certified Information Systems Security Professional

Sample Statistics showing number of threats over time and the origination.

Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004

TROY A. NEWMAN

CISSP Certified Information Systems Security Professional

A sample detailed log showing the alert type and action as well as the source IP address/port and attempted exploit.
This data is used to set additional security measures.

Security Center the last month

Search events | Filter | 1077 matching events

Summary **Events**

Time	Type	Source	Destination	Disposition	Action	
Nov 7 12:49:46	IDS Alert	5.188.10.251:59828	-SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:46	IDS Alert	5.188.10.251:59828	-SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:40	IDS Alert	5.188.10.251:52846	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:40	IDS Alert	5.188.10.251:52846	-SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:38	IDS Alert	5.188.10.251:51936	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:38	IDS Alert	5.188.10.251:51936	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:37	IDS Alert	5.188.10.251:50520	-SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:37	IDS Alert	5.188.10.251:50520	-SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:35	IDS Alert	5.188.10.251:49204	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:35	IDS Alert	5.188.10.251:49204	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:34	IDS Alert	5.188.10.251:47566	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:34	IDS Alert	5.188.10.251:47566	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:33	IDS Alert	5.188.10.251:46084	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:33	IDS Alert	5.188.10.251:46084	-SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:31	IDS Alert	5.188.10.251:44744	-SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:31	IDS Alert	5.188.10.251:44744	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:30	IDS Alert	5.188.10.251:43292	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:30	IDS Alert	5.188.10.251:43292	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:28	IDS Alert	5.188.10.251:41638	-SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:28	IDS Alert	5.188.10.251:41638	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt
Nov 7 12:49:27	IDS Alert	5.188.10.251:40468	SERVER Windows Vista		Blocked	Apache Struts remote code execution attempt

TROY A. NEWMAN

CISSP Certified Information Systems Security Professional

Sample AV Report Dashboard:
Centrally managed AV with alerting mechanism.
Alerts to device not seen, threat detected, version control.

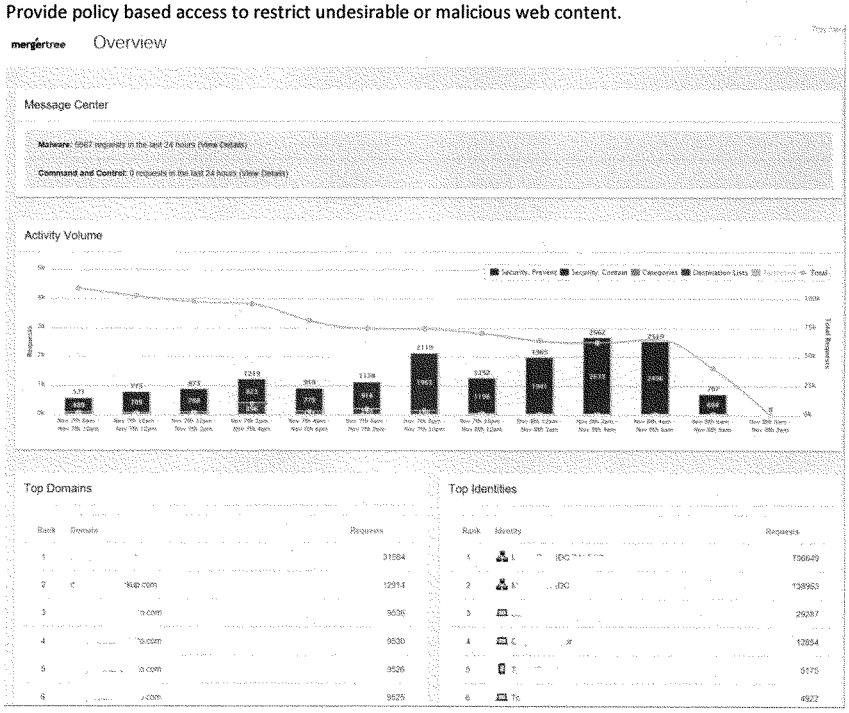
	Hostname	Policy	Group	Status	Last Seen	Last Threat	Agent Version
3		Recommended Defaults	Default Group	Not Seen Recently	Aug 24th 2017, 19:29	Jul 25th 2017, 15:49	9.0.17.28
6		Recommended Defaults		Not Seen Recently	Oct 13th 2017, 17:32		9.0.18.34
7		Recommended Defaults		Protected	Nov 8th 2017, 09:01		9.0.18.34
8		Recommended Defaults		Protected	Nov 7th 2017, 13:28	Oct 11th 2017, 09:27	9.0.18.34
9		Recommended Defaults	Default Group	Protected	Nov 8th 2017, 09:41		9.0.18.34
10		Recommended Defaults	Default Group	Protected	Nov 8th 2017, 09:05		9.0.18.34
11		Recommended Defaults	Default Group	Protected	Nov 8th 2017, 01:37	Aug 21st 2017, 07:14	9.0.18.34
12		Recommended Defaults	Default Group	Protected	Nov 8th 2017, 09:39	Oct 9th 2017, 10:50	9.0.18.34
13		Capital Royalty Temp		Protected	Nov 7th 2017, 12:07	Nov 8th 2014, 16:58	9.0.18.34
14		Capital Royalty Temp		Protected	Nov 8th 2017, 09:08		9.0.18.34
15		Inukalty	Default Group	Protected	Nov 7th 2017, 10:03	Jul 17th 2017, 17:07	9.0.18.34
16		Recommended Defaults	Default Group	Protected	Nov 8th 2017, 09:05	Jun 21st 2016, 09:09	9.0.18.34
17		Capital Royalty Temp		Protected	Nov 8th 2017, 03:05	Sep 3rd 2016, 10:23	9.0.18.34
18		Recommended Defaults	Default Group	Protected	Nov 7th 2017, 19:55	May 11th 2016, 16:02	9.0.18.34
19		Recommended Defaults		Protected	Nov 7th 2017, 19:12	May 4th 2017, 09:42	9.0.18.34
20		Recommended Defaults	Default Group	Protected	Nov 8th 2017, 07:46	Jun 12th 2017, 08:14	9.0.18.34
21		Recommended Defaults	Default Group	Protected	Nov 8th 2017, 08:59		9.0.18.34
22		Recommended Defaults	Default Group	Protected	Nov 7th 2017, 23:57	May 24th 2017, 09:56	9.0.18.34
23		Recommended Defaults		Protected	Nov 4th 2017, 18:29	Aug 24th 2015, 09:26	9.0.18.34
24		Recommended Defaults		Protected	Nov 8th 2017, 08:03	May 2nd 2017, 12:28	9.0.18.34
25		Recommended Server Defaults		Protected	Nov 8th 2017, 09:04		9.0.18.34
26		Recommended Server Defaults		Protected	Nov 7th 2017, 13:28		9.0.18.34
27		Recommended Server Defaults		Protected	Nov 8th 2017, 09:04	Sep 15th 2014, 09:46	9.0.18.34
28		All Console Access		Protected	Nov 8th 2017, 09:53	Dec 29th 2014, 09:51	9.0.18.34

Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004

TROY A. NEWMAN

CISSP Certified Information Systems Security Professional

Sample Secure DNS Report: Should be available on all networks using secure DNS
Identify potential malware threats seeking connections back to command and control.
Prevent connections to known bad networks.
Provide policy based access to restrict undesirable or malicious web content.



Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004

TROY A. NEWMAN

CISSP Certified Information Systems Security Professional

In closing, I have attempted to articulate the high points for consideration. There are, of course, much greater levels of technical detail required for execution. The process begins with the assessment phase. We need to understand the full scale of this threat. Network monitoring systems currently in use should be reviewed for traffic to Kaspersky Labs and other foreign networks. Immediate restriction of access to specific foreign IP space is also recommended. The only way to be certain that the systems are completely remediated is by replacing the hard drives. Removed hard drives require secure disposal processes.

The scale of this task is enormous. Effective remediation of this issue and implementation of ongoing cybersecurity practices will require resources across our nation. As a corporate executive of a cybersecurity company, I am privileged to participate in a peer network of managed service providers with a national reach. I suggest the committee consider leveraging the resources of Managed Service Providers with geographic proximity to local agency offices to accomplish the task of remediation and implementation within the preset time frame of DHS BOD 17-01. This would engage our local community businesses with their local government agencies guided with oversight from the DHS.

Technology drives our economy and improves our lives. Our nation is founded upon free enterprise and American ingenuity. What is as stake is no less than our intellectual property and potentially government classified information. We must find a balance in security, integrity, and freedom. As we protect our geographical borders we must also protect our cyberspace borders to ensure the safety and liberty of our fellow citizens.

Cyber5, LLC
18 Augusta Pines Dr. Suite 150E
Spring, Texas 77389
713.982.8004