AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

IT SUPPLY CHAIN SECURITY: REVIEW OF GOVERNMENT AND INDUSTRY EFFORTS

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MARCH 27, 2012

Serial No. 112–131

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

77–892 PDF WASHINGTON : 2013

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

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

CLIFF STEARNS, Florida
Chairman

LEE TERRY, Nebraska
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
CORY GARDNER, Colorado
H. MORGAN GRIFFITH, Virginia
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

DIANA DEGETTE, Colorado
Ranking Member
JANICE D. SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
KATHY CASTOR, Florida
EDWARD J. MARKEY, Massachusetts
GENE GREEN, Texas
CHARLES A. GONZALEZ, Texas
DONNA M. CHRISTENSEN, Virgin Islands
JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

	Page
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	1
Prepared statement	4
Hon. Diana DeGette, a Representative in Congress from the State of Colorado, opening statement	6
Hon. Tim Murphy, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	7

WITNESSES

Gregory C. Wilshusen, Director of Information Security Issues, Government Accountability Office	9
Prepared statement	11
Mitchell Komaroff, Director, Trusted Mission Systems and Networks, Department of Defense	24
Prepared statement	26
Gil Vega, Associate Chief Information Officer for Cybersecurity and Chief Information Security Officer, Department of Energy	39
Prepared statement	41
Insert for the record	60
Lawrence Castro, Managing Director, The Chertoff Group	64
Prepared statement	66
Dave Lounsbury, Chief Technology Officer, The Open Group	71
Prepared statement	73

SUBMITTED MATERIAL

Report, dated March 2012, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," Government Accountability Office, submitted by Mr. Stearns [1] .....

[1] The report is available at http://www.gao.gov/products/GAO-12-361.

IT SUPPLY CHAIN SECURITY: REVIEW OF GOVERNMENT AND INDUSTRY EFFORTS

TUESDAY, MARCH 27, 2012

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:04 a.m., in room 2123, Rayburn House Office Building, Hon. Cliff Stearns (chairman of the subcommittee) presiding.

Present: Representatives Stearns, Terry, Myrick, Murphy, Bilbray, Gingrey, Scalise, Griffith, Barton, DeGette, and Green.

Staff Present: Carl Anderson, Counsel, Oversight; Sean Bonyun, Deputy Communications Director; Karen Christian, Deputy Chief Counsel, Oversight; Andy Duberstein, Deputy Press Secretary; Andrew Powaleny, Deputy Press Secretary; Krista Rosenthall, Counsel to Chairman Emeritus; Alan Slobodin, Deputy Chief Counsel, Oversight; Lyn Walker, Coordinator, Admin/Human Resources; Alex Yergin, Legislative Clerk; Alvin Banks, Democratic Investigator; Tiffany Benjamin, Democratic Investigative Counsel; and Brian Cohen, Democratic Investigations Staff Director and Senior Policy Advisor.

Mr. STEARNS. Good morning, everybody. I call to order this subcommittee's third hearing on cybersecurity.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

With the growing reliance on the global economy for our goods and services, we are faced with the challenge that ensuring the security of those items has become even more difficult. As the global economy grows, so does the complexity of the global supply chain. The U.S. Government is increasingly reliant on commercially available products for information technology, IT services, and components. This reliance forces the U.S. Government to depend on the trustworthiness of the global commercial supply chain. Cyber or state-sponsored actors are capable of secretly inserting malicious code into both hardware and software during the manufacture of those items. Let me give you some specific examples:

In July 2010, Dell announced that some of its PowerEdge motherboards contain malicious spyware that gathered information about a victim's Internet browsing habits and collected personally identifiable information.

During a security conference in May 2010, IBM gave complimentary USB drives to attendees that contained two kinds of malware, including a keylogger program.

In March 2010, the Spanish cell phone company Vodafone released a new version of a popular smartphone infected with a version of the Butterfly botnet in addition to other malicious software.

These, my colleagues, and many other instances of supply chain poisoning are capable of causing damage to, allowing a cyber criminal unauthorized access to, or allowing the exfiltration of sensitive or personally identifiable information from a victim's computer system.

Now, last week, the Government Accounting Office released a report examining the risk and threats to the supply chains of both commercial and Federal IT systems. The GAO studied four agencies involved in national security: Department of Defense, Energy, Homeland Security, and Justice and their ability to access the risk to their own IT supply chains and the steps they have taken to mitigate them. We are joined by the GAO today to discuss their findings and recommendations.

While DOD and DOE and DHS and Justice each participated in interagency efforts to address supply chain security, some of these agencies had been more progressive than others in addressing IT supply chain security risks. In particular, I was troubled to find that the GAO concluded that the Department of Energy had not—had not developed clear policy that defined what security measures it needed to protect against supply chain threats. Clearly defined security measures with comprehensive implementing procedures are necessary and vital to the protection of Federal IT.

One additional comment about the report, as a whole, is that there appears to be no integrated response amongst the Federal IT enterprise to address supply chain risks. Agencies are left to their own devices to address this risky and complex threat. I find this very troubling.

Today, we will hear testimony from two panels of witnesses. On our first panel, we are joined by Mr. Gregory Wilshusen, Director of Information Security Issues at GAO and his staff who assisted in drafting this report. We are also joined by representatives of two agencies who are the subject of the report, Mr. Mitchell Komaroff, Director of the Trusted Mission Systems and Network at the Department of Defense, and Mr. Gil Vega, Associate CIO for Security and Chief Information Security Officer at the Department of Energy.

I look forward to their testimony and getting a much better understanding of the work they do to ensure the integrity of their agency's IT supply chain.

I also want to welcome our second panel of witnesses who will provide us with an overview of the private-sector approach to identifying IT supply chain risk and using industry's best practices to mitigate them.

We are joined by Mr. Larry Castro, Managing Director at the Chertoff Group and former National Security Agency Central Security Services representative to the U.S. Department of Homeland

Security. Also joining us is Dave Lounsbury, Chief Technological Officer at The Open Group and International IT Standards Board.

We welcome all of the second panel, also.

As I mentioned previously, this is the subcommittee's third hearing in this Congress on cybersecurity. The purpose of this hearing in particular is to understand the threats and vulnerabilities to Federal IT supply chains and how best to ensure their integrity. I have enjoyed working with the ranking member on this matter and the minority in particularly and look forward to our continuing cooperation on cybersecurity issues; and I yield to the distinguished ranking member, Ms. DeGette from Colorado.

[The report is available at http://www.gao.gov/products/GAO-12-361.]

[The prepared statement of Mr. Stearns follows:]

Opening Statement of the Honorable Cliff Stearns
Subcommittee on Oversight and Investigations
Hearing on "IT Supply Chain Security: Review of Government and Industry Efforts"
March 27, 2012
(*As prepared for delivery*)

With the growing reliance on the global economy for our goods and services, we are faced with the challenge that ensuring the security of those items has become ever more difficult. As the global economy grows, so does the complexity of the global supply chain. The U.S. Government is increasingly reliant on commercially available products for information technology (IT) services and components. This reliance forces the U.S. Government to depend on the trustworthiness of the global commercial supply chain.

Cyber or state-sponsored actors are capable of secretly inserting malicious code into both hardware and software during the manufacture of those items. For example:

- In July 2010, Dell announced that some of its PowerEdge motherboards contained malicious spyware that gathered information about a victim's Internet browsing habits and collected personally identifiable information.

- During a security conference in May 2010, IBM gave complimentary USB drives to attendees that contained two kinds of malware, including a keylogger program.

- In March of 2010, Spanish Cell Phone company, Vodafone, released a new version of a popular smartphone infected with a version of the Butterfly botnet, in addition to other malicious software.

These and many, many other instances of supply chain poisoning are capable of causing damage to, allowing a cyber criminal unauthorized access to, or allowing the exfiltration of sensitive or personally identifiable information from a victim's computer system.

Late last week, the Government Accountability Office released a report examining the risk and threats to the supply chains of both commercial and federal IT systems. The GAO studied four agencies involved in national security — the Departments of Defense, Energy, Homeland Security, and Justice — and their ability to assess the risk to their own IT supply chains and the steps they have taken to mitigate them. We are joined by the GAO today to discuss their findings and recommendations.

While DOD, DOE, DHS, and Justice each participate in interagency efforts to address supply chain security, some of these agencies have made more progress than others in addressing IT supply chain security risks. In particular, I was troubled to find that the GAO concluded that the Department of Energy had not developed clear policies that define what security measures are needed to protect against supply chain threats. Clearly defined security measures with comprehensive implementing procedures are necessary and vital to the protection of federal IT. One additional comment about the report as a whole is that there appears to be no

integrated response amongst the federal IT enterprise to address supply chain risks. Agencies are left to their own devices to address this risky and complex threat. I find this troubling.

Today, we will hear testimony from two panels of witnesses. On our first panel, we are joined by Mr. Gregory Wilshusen, Director of Information Security Issues at GAO and his staff who assisted in drafting the report. We are also joined by representatives of two agencies who are the subjects of the report. Mr. Mitchell Komaroff, Director of the Trusted Mission Systems Networks at the Department of Defense and Mr. Gil Vega, Associate CIO for Cybersecurity & Chief Information Security Officer at the Department of Energy. I look forward to their testimony, and getting a better understanding of the work they do to ensure the integrity of their agencies' IT supply chain.

I also want to welcome our second panel of witnesses who will provide us with an overview of the private sector approach to identifying IT supply chain risks and using industry best practices to mitigate them. We are joined by Mr. Larry Castro, Managing Director at The Chertoff Group and former National Security Agency/Central Security Service Representative to the US Department of Homeland Security (DHS). Also joining us is Dave Lounsbury, Chief Technology Officer at The Open Group an international IT standards board. Welcome to all of you.

As I mentioned previously, this is the subcommittee's third hearing in this Congress on cybersecurity. The purpose of this hearing, in particular, is to understand the threats and vulnerabilities to federal IT supply chains and how best to ensure their integrity. I have enjoyed working with Ranking Member DeGette and the Minority in these matters and look forward to our continued cooperation on cybersecurity issues.

###

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Thank you very much, Mr. Chairman. I also appreciate the work that you have done on this issue and working with the minority.

Ensuring the integrity of our information technology supply chain is critical to protecting our Federal systems against terrorists, counterfeiters, hackers, and other enemies. In 1997, the Government Accountability Office made government-wide information security part of its biannual high-risk series. Since then, the government, like the private sector, has become more and more technology dependent and more and more reliant on private-sector hardware and software.

Just to think of one example, think about how the census worked 2 years ago. What used to be collected versus pad and paper is now collected and transmitted electronically.

And with every new technology our Nation's infrastructure becomes more exposed to new threats and vulnerabilities. As more components are manufactured outside of this country, our technology systems become more vulnerable to infiltration by our foreign enemies. A few malicious lines of software code, cleverly hidden in a larger program, counterfeit hardware or software, and even malicious or unqualified service providers all present risk to the technology that drives our supply chain.

In January of this year, President Obama launched the National Strategy for Global Supply Chain Security. I commend the President for taking supply chain issues seriously, but we as Congress also have an important role to play in ensuring the security and safety of these systems.

Last month, as the chairman mentioned, this subcommittee held a hearing on cybersecurity threats to our electric grid. During that hearing, I asked our witnesses about the potential risk to the supply chain associated with devices connected to the grid. Richard Campbell, testifying on behalf of the Congressional Research Service, agreed if the wrong people were able to get improper access to these devices, they could do any number of dangerous things, including implanting a software bug in a smart meter's firmware and control its functions and the functions of the devices attached to it. A meter could be set, for example, to control the thermostat for a room containing servers, and a hacker could increase the temperature to destroy the servers.

We know that counterfeit circuitry can cause critical devices or systems to malfunction. Logic bombs can be inserted into devices. These are systems that will lie dormant until a device engages in a certain activity, at which point they can overtake the device and any system associated with it.

Our Federal Government, including the military, and the Department of Homeland Security is heavily reliant on the private sector to provide these devices and to vet them to ensure they are safe and secure. GAO's findings suggest that some of the agencies like the Department of Defense are on the right track to safeguarding their information systems from external threats, but other agencies, like the Department of Energy, still need to define supply line

chain protection measures and develop implementing procedures and monitoring capabilities.

However, this isn't just an issue for Federal agencies. Private companies also struggle to develop plans to prevent and respond to supply chain disruptions. That is why I am pleased to have the second panel here today to talk about how the private sector is addressing these issues. I look forward to learning about the threats and vulnerabilities they see in the hardware and the software systems companies purchase and sell and also what private companies are doing to ensure the products they provide to their customers are protected.

In the cybersecurity context, we know that companies are not required to report these threats and vulnerabilities to the Federal Government, and we are aware that in certain instances companies have chosen not to do so, leaving Federal agencies in the dark about how widespread a problem is or whether it has been resolved. We need to hold everybody accountable for ensuring that our supply chain is safe, and that starts with ensuring that those who build and sell key supply chain hardware and software components are properly safeguarding their devices from threats.

We must find ways to ensure that U.S. Suppliers are responsible for the security of their foreign-made devices and systems. We must make sure that manufacturers are reporting threats, vulnerabilities, and cyber attacks quickly so that the government and the private sector can take appropriate actions. And, finally, we must make sure that the Federal Government is carefully vetting the information technology products they purchase.

Mr. Chairman, I look forward to hearing from both of the panels about what work we can do to ensure our Federal technologies are as secure as possible; and I yield back the balance of my time.

Mr. STEARNS. Thank you, gentlelady; and I recognize Mr. Murphy. The gentleman from Pennsylvania is recognized for an opening statement.

OPENING STATEMENT OF HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. MURPHY. Yes, thank you, Mr. Chairman.

On December 11, 1941, despite some warnings of what was to come and despite seeing clear planes flying towards Pearl Harbor, we slept. As the Korean war started, an intelligence lapse also meant that South Korea was overwhelmed. And when the Marine barracks in Lebanon were bombed, it occurred in the midst of dozens, perhaps hundreds of warnings that something was about to occur. We are now facing similar threats in the area of cybersecurity, and it is important that we do not sleep as this dawn is upon us.

When we look at a measure of cybersecurity, such things as resilience, an ability to send out an alert, defending against an attack, being able to launch a counterattack and recover from an attack, unfortunately, many of the sectors that we know of, inagriculture and food, military, transportation, health, finance, banking, telecommunication, and energy, are all woefully inadequate in how they can act.

Our country is at war with an enemy we cannot see, but the battle has the potential to inflict an incalculable amount of damage on our economy, our national defense, and families. A looming terrorist attack may not come in the form of a hijacked plane hitting a building but from a terrorist cell lurking inside of our computers at work and at home, ready to strike our banks or energy grid and other sectors.

Cyber terrorists and hackers are not just unaffiliated rogue actors. They are highly trained special operations agents being employed by foreign countries.

These startling developments and how the cyber war is evolving were revealed to me this past summer when I sat on a special cybersecurity task force formed by Speaker Boehner. These threats from abroad can manifest themselves in mysterious ways. Consider the potential weaknesses in our national security when the Marine Corps, Air Force, Federal Aviation Administration, and Federal Bureau of Investigation purchased counterfeit Cisco products that originated in China. Or that Beijing's military apparatus is tightening its reign over the country's technology sector, when we realize the People's Liberation Army has formed IT workers into so-called cyber militias within thousands of companies across China.

The threat of foreign nations waging cyber warfare against the United States is so real that the Defense Department is raising red flags about Huawei Technologies, the world's largest manufacturer of computer hardware, acquiring Symantec, a security company whose software is installed on computers at homes, business, and Federal agencies across the country.

We have to make sure that we are on alert for all levels of cybersecurity and following the IT purchasing line all the way through as well as monitoring software and people's access to our computers. This threat is very real, and it is very active in our country and around the world. Failure to act means, once again, at dawn we sleep.

And with that I yield back.

Mr. STEARNS. The gentlemen yields back.

I don't see anyone on the minority side, so we will go right to the first panel.

As you know, the testimony that you are about to give is subject to Title 18, Section 1001 of the United States Code. When holding an investigative hearing, this committee has a practice of taking testimony under oath. Do you have any objection to testifying under oath?

PANEL. No.

Mr. STEARNS. The chair then advises you that under the rules of the House and rules of the committee you are entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony today?

PANEL. No.

Mr. STEARNS. In that case, will you please rise and raise your right hand, and I will swear you in.

[Witnesses sworn.]

Mr. STEARNS. We now welcome each of you to give your 5-minute summary of your written statement. Start with you.

STATEMENTS OF GREGORY C. WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; MITCHELL KOMAROFF, DIRECTOR, TRUSTED MISSION SYSTEMS AND NETWORKS, DEPARTMENT OF DEFENSE; AND GIL VEGA, ASSOCIATE CHIEF INFORMATION OFFICER FOR CYBERSECURITY AND CHIEF INFORMATION SECURITY OFFICER, DEPARTMENT OF ENERGY

STATEMENT OF GREGORY WILSHUSEN

Mr. WILSHUSEN. Chairman Stearns, Ranking Member DeGette, and members of the subcommittee, thank you for the opportunity to testify at today's hearing on IT supply chain security.

Mr. STEARNS. I think you have to—do you have the mic on?

Mr. WILSHUSEN. Yes, I do.

Mr. STEARNS. Just move it a little closer. That would be good.

Ms. DEGETTE. You need to put it close.

Mr. WILSHUSEN. OK.

Thank you for the opportunity to testify at today's hearing on IT supply chain security.

IT systems and the products and services that support them are essential to the operations of the Federal Government. These products and services are created and delivered through a complex global supply chain that involves a multitude of organizations, individuals, activities, and resources.

My testimony today summarizes the contents of our recently issued report on IT supply chain risks and the extent to which the Departments of Energy, Homeland Security, Justice, and Defense have addressed these risks. But if I may first, Mr. Chairman, recognize some members of my team whose dedication and professionalism were instrumental to the development of this report.

And this is Mike Gilmore.

Mr. STEARNS. What is Mike Gilmore's title? Can you give the title?

Mr. WILSHUSEN. He is an assistant director for IT.

Mr. STEARNS. OK.

Mr. WILSHUSEN. R.J. Hagerman, who is an analyst, and Kush Malhotra, who is also the analyst in charge for our engagement.

Mr. STEARNS. Thank you.

Mr. WILSHUSEN. In addition, there are two members who are not here, Brad Becker and Lee McCracken, who are back in their offices, who also played a key role.

Mr. Chairman, the exploitation of IT products and services through the supply chain is an emerging threat. IT supply chain-related threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services. These threats include the insertion of harmful or malicious software and hardware, installation of counterfeit items, disruption in the production or distribution of critical products, reliance on unqualified or malicious service providers, and installation of software and hardware containing unintentional vulnerabilities.

These threats can be exercised by exploiting vulnerabilities that could exist at multiple points in the supply chain. Examples of such vulnerabilities include acquiring products or parts from unauthorized distributors, using insecure transportation, storage, or de-

livery mechanisms, and installing hardware and software without sufficiently inspecting or testing them.

These threats and vulnerabilities can potentially lead to a range of harmful effects, including allowing attackers to take control of systems or decreasing the availability of critical materials needed to develop or operate systems.

The Departments of Energy, Homeland Security, Justice, and Defense varied in the extent to which they have addressed supply chain risks. Each of the four agencies participated in one or more interagency efforts to address supply chain security, such as developing technical and policy tools, collaborating with the intelligence community, and participating in the Comprehensive National Cybersecurity Initiative on supply chain risk management. These efforts are key to understanding and addressing global supply chain risk.

However, with respect to establishing supply chain protection measures for their internal departmental systems, three of the agencies had not fully addressed Federal guidelines. These guidelines recommend that agencies, for their high-impact systems, define supply chain-related protection measures, develop procedures for implementing them, and monitor their effectiveness.

However, Energy and Homeland Security had not yet taken these steps; and while Justice has defined supply chain protection measures, including a foreign ownership, control, and influence review, it had not yet developed implementing procedures or monitoring capabilities.

The Department of Defense, on the other hand, has made greater progress. It has defined policies, requires program protection plans, issued a key practices and implementation guide, conducted pilot programs, and implemented a monitoring mechanism to determine the status and effectiveness of its supply chain protection pilots.

In our recently issued report, we recommended that the Departments of Energy, Homeland Security, and Justice take steps as needed to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk to their internal systems. The departments generally agreed with our recommendations.

In summary, Mr. Chairman, the global IT supply chain introduces risk that, if realized, could jeopardize the confidentiality, integrity, and availability of Federal information systems and adversely impact an agency's operations, assets, and employees. This risk highlights the importance for Federal agencies to take appropriate actions to develop, document, and implement the policies, procedures, and controls necessary to cost-effectively manage the associated risk.

Mr. Chairman, Ms. DeGette, this concludes my statement. I would be happy to answer any questions at the appropriate time.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, March 27, 2012

IT SUPPLY CHAIN

Additional Efforts Needed by National Security-Related Agencies to Address Risks

Statement of Gregory C. Wilshusen, Director
Information Security Issues

GAO-12-579T

Highlights of GAO-12-579T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

March 27, 2012

IT SUPPLY CHAIN

Additional Efforts Needed by National Security-Related Agencies to Address Risks

Why GAO Did This Study

Information technology (IT) systems and the products and services that support them are essential to the operations of the federal government. These products and services are delivered through a complex global supply chain, and the exploitation of vulnerabilities in the IT supply chain is an emerging threat. Federal law requires establishment of information security programs, and implementing standards and guidelines provide for managing supply chain risk.

GAO was asked to testify on its recently issued report that, among other things, identified key risks associated with the supply chains used by federal agencies to procure IT equipment, software, and services, and assessed the extent to which four national security-related agencies have addressed such risks. In producing that report, GAO analyzed federal acquisition and information security laws, regulations, standards, and guidelines; examined departmental policies and procedures; and interviewed officials from four national security-related departments, the intelligence community, and nonfederal entities.

What GAO Recommends

In its report, GAO recommended that the Departments of Energy, Homeland Security, and Justice take steps, as needed, to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk. In commenting on a draft of the report, the departments generally concurred with the recommendations.

What GAO Found

Reliance on a global supply chain introduces multiple risks to federal information systems and underscores the importance of threat assessments and mitigation. Supply chain threats are present at various phases of a system's development life cycle and could create an unacceptable risk to federal agencies. Key supply chain-related threats include

- installation of intentionally harmful hardware or software (i.e., containing "malicious logic");
- installation of counterfeit hardware or software;
- failure or disruption in the production or distribution of critical products;
- reliance on malicious or unqualified service providers for the performance of technical services; and
- installation of hardware or software containing unintentional vulnerabilities, such as defective code.

These threats can have a range of impacts, including allowing attackers to take control of systems or decreasing the availability of critical materials needed to develop systems. These threats can be introduced by exploiting vulnerabilities that could exist at multiple points in the supply chain. Examples of such vulnerabilities include acquisition of products or parts from unauthorized distributors; application of untested updates and software patches; acquisition of equipment, software, or services from suppliers without knowledge of their past performance or corporate structure; and use of insecure delivery or storage mechanisms. These vulnerabilities could by exploited by malicious actors, leading to the loss of the confidentiality, integrity, or availability of federal systems and the information they contain.

The four national security-related agencies in GAO's review—the Departments of Energy, Homeland Security, Justice, and Defense—varied in the extent to which they have addressed supply chain risks. Specifically, Energy and Homeland Security had not yet defined supply chain protection measures for department information systems and are not in a position to develop implementing procedures and monitoring capabilities. Justice has defined supply chain protection measures but has not developed implementation procedures or monitoring capabilities. Until these agencies develop comprehensive policies, procedures, and monitoring capabilities, increased risk exists that they will be vulnerable to IT supply chain threats. By contrast, the Department of Defense has made greater progress: it has defined supply chain protection measures and implementing procedures and initiated efforts to monitor compliance and effectiveness. In addition, various interagency efforts are under way to address supply chain risks affecting federal IT.

View GAO-12-579T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on federal and industry efforts related to information technology (IT) supply chain security. As you know, information systems and the products and services that support them are essential for government operations. Federal agencies rely extensively on computerized information systems and electronic data to carry out their operations, and securing these systems and data is essential to protecting national and economic security.

As commerce has become more globalized, the supply chain for IT and services has become increasingly complex.[1] This complexity, in turn, creates potential vulnerabilities that can be exploited by cyber threats, potentially degrading the confidentiality, integrity, and availability of critical and sensitive networks, IT-enabled equipment, and data. These threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services and can appear at each phase of the IT system development life cycle. In January 2012, the Director of National Intelligence identified the vulnerabilities associated with the IT supply chain for the nation's networks as one of the greatest strategic cyber threat challenges the country faces.[2] In addition, we have identified the protection of federal information systems as a governmentwide high-risk area since 1997.[3]

My testimony today summarizes the contents of our recently issued report on IT supply chain risks, which, among other things, identified key risks associated with the supply chains used by federal agencies to procure IT equipment, software, or services, and assessed the extent to which four

[1]The National Institute of Standards and Technology (NIST) has defined the term "supply chain" to mean a set of organizations, people, activities, information, and resources for creating and moving a product or service from suppliers through to an organization's customers. Also, NIST defines "information technology" as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes, among other things, computers, software, firmware, and services (including support services).

[2]Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," unclassified statement for the record before the Senate Select Committee on Intelligence (Washington, D.C.: Jan. 31, 2012).

[3]See, most recently, GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

national security-related agencies have addressed such risks.[4] In preparing this statement in March 2012, we relied on the work supporting this report. In producing that report, we analyzed federal acquisition and information security laws, regulations, standards, and guidelines; examined departmental policies and procedures; and interviewed officials from four national security-related departments, the intelligence community, and nonfederal entities. The report contains a more detailed overview of the scope of our review and the methodology used. The work on upon which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

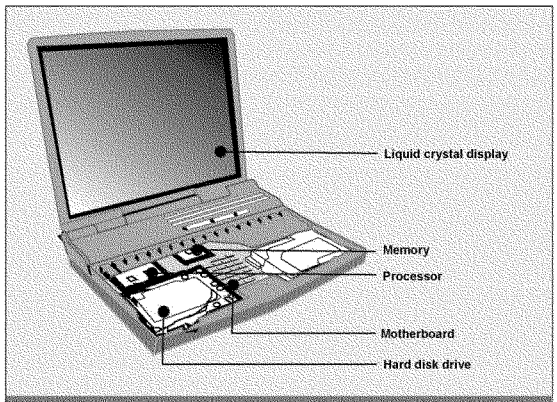
Information systems can be complex undertakings consisting of a multitude of pieces of equipment and software products, and service providers. Each of these components may rely on one or more supply chains. Obtaining a full understanding of the sources of a given information system can also be extremely complex. According to the Software Engineering Institute, the identity of each product or service provider may not be visible to others in the supply chain. Typically, an acquirer, such as a federal agency, will only know about the participants directly connected to it in the supply chain. In addition, the complexity of corporate structures, in which a parent company (or its subsidiaries) may own or control companies that conduct business under different names in multiple countries, presents additional challenges to fully understanding the sources of an information system. As a result, the acquirer will have little visibility into the supply chains of its suppliers.

Federal procurement law and policies promote the acquisition of commercial products when they meet the government's needs. Commercial providers of IT use a global supply chain to design, develop, manufacture, and distribute hardware and software products throughout the world. Many of the manufacturing inputs required for those products—whether physical materials or knowledge—are acquired from various

[4]GAO, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: Mar. 23, 2012).

sources around the globe. Figure 1 depicts the potential countries of origin of common suppliers of various components within a commercially available laptop computer.

Figure 1: Potential Origins of Common Suppliers of Laptop Components



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information.

Federal Law Requires Establishment of Information Security Programs, and Implementing Standards and Guidelines Provide for Managing Supply Chain Risk

The Federal Information Security Management Act of 2002 (FISMA) establishes federal agency information security program requirements that support the effectiveness of information security controls over

information resources that support federal operations and assets.[5] Its framework creates a cycle of risk management activities necessary for an effective security program, and it assigns responsibilities to the National Institute of Standards and Technology (NIST) for providing standards and guidelines on information security.[6]

In its August 2009 revision of Special Publication (SP) 800-53 (Revision 3), which provides recommended security controls for federal agencies and organizations,[7] NIST included for the first time a security control for supply chain protection (SA-12).[8] SA-12 identified several specific measures organizations could use to provide additional supply chain protections, such as conducting due diligence reviews of suppliers; using trusted shipping and warehousing; and employing independent analysis and penetration testing of IT systems, components, and products. In addition, SP 800-53, Revision 3, includes a security control for system and service acquisition policies and procedures (SA-1).[9] Thus, for systems where both controls are selected, agencies should develop, disseminate, and review acquisition policy and implementing procedures that help protect against supply chain threats throughout the system development life cycle.[10] Further, in March 2011, NIST published SP 800-

[5]Title III of the E-Government Act of 2002, Pub. L. No. 107-347, Dec. 17, 2002.

[6]FISMA requires that federal agencies comply with NIST information security standards, and agencies may not waive their use. In addition, FISMA requires agencies to develop, document, and implement agencywide programs to provide security for the information systems that support their operations and assets.

[7]NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 3 (Gaithersburg, Md.: May 2010).

[8]SA-12 states that an organization should define and employ a list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy. According to SP 800-53, Revision 3, SA-12 should be selected for the initial control baseline of all agency information systems categorized as high impact.

[9]SA-1 states that organizations should develop formal, documented procedures to facilitate the implementation of system and services acquisition policy and associated system and services acquisition family of controls, which includes SA-12. According to SP 800-53, Revision 3, SA-1 should be selected for the initial control baseline regardless of categorization.

[10]These controls are required for both non-national security and national security systems. Specifically, OMB requires federal agencies to use SP 800-53 for selecting controls for non-national security systems, while the Committee on National Security Systems, a committee established to issue policy directives and instructions on information security for national security systems, has established SP 800-53 as a common foundation for information security controls for national security systems.

39, an approach to organizationwide management of information security risk, which states that organizations should monitor risk on an ongoing basis as part of a comprehensive risk management program.[11]

IT Supply Chain Presents Numerous Information Security Risks to Federal Agencies

Reliance on a global supply chain introduces multiple risks to federal information systems and underscores the importance of threat assessments and risk mitigation. Supply chain threats are present at various phases of a system's development life cycle. Key threats that could create an unacceptable risk to federal agencies include the following:

- installation of hardware or software containing malicious logic, which is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose;
- installation of counterfeit hardware or software, which is hardware or software containing non-genuine component parts or code;
- failure or disruption in the production or distribution of critical products resulting from manmade or natural causes;
- reliance on a malicious or unqualified service provider for the performance of technical services; and
- installation of hardware or software that contains unintentional vulnerabilities, such as defects in code that can be exploited.

Such threats can have a range of impacts, including allowing attackers to take control of systems and read, modify, or delete sensitive information; decreasing the reliability of IT equipment; decreasing the availability of material needed to develop systems; or allowing remote attackers to cause a denial of service, among other things.

Threat actors can introduce these threats into federal information systems by exploiting vulnerabilities that could exist at multiple points in the global supply chain. In addition, supply chain vulnerabilities can include weaknesses in agency acquisition or security procedures, controls, or implementation related to an information system. Examples of types of vulnerabilities that could be exploited include

[11]NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: March 2011).

- acquisition of IT products or parts from sources other than the original manufacturer or authorized reseller, such as independent distributors, brokers, or on the gray market;
- applying untested updates and software patches to information system components;
- acquiring equipment, software, or services from suppliers without understanding their past performance or corporate structure; and
- using delivery or storage mechanisms that are not secure.

If a threat actor exploits an existing vulnerability, it could lead to the loss of the confidentiality, integrity, or availability of the system and associated information.

Three National Security-Related Agencies Have Not Fully Addressed IT Supply Chain Risk

Although the four agencies in our review—the Departments of Energy, Homeland Security (DHS), Justice, and Defense—have acknowledged the risks presented by supply chain vulnerabilities, they varied in the extent to which they have addressed these risks by (1) defining supply chain protection measures for department information systems, (2) developing implementing procedures for these measures, and (3) establishing capabilities for monitoring compliance with and the effectiveness of such measures.

Three of the four departments have made limited progress in addressing supply chain risk:

- In May 2011, the Department of Energy revised its information security program, which requires Energy components to implement provisions based on NIST and Committee on National Security Systems guidance. However, the department was unable to provide details on implementation progress, milestones for completion, or how supply chain protection measures would be defined. Because it had not defined these measures or associated implementing procedures, the department was also not in a position to monitor compliance or effectiveness.
- Although its information security guidance mentions the NIST control related to supply chain protection, DHS has not defined the supply chain protection measures that system owners should employ. The department's information security policy manager stated that it was in the process of developing policy that would address supply chain protection, but did not provide details on when it would be completed. In addition, in the absence of such a policy, DHS was not in a position

to develop implementation procedures or to monitor compliance or effectiveness.

- The Department of Justice has defined specific security measures for protecting against supply chain threats through the use of provisions in vendor contracts and agreements. Officials identified (1) a citizenship and residency requirement and (2) a national security risk questionnaire as two provisions that address supply chain risk. However, Justice has not developed procedures for ensuring the effective implementation of these protection measures or a mechanism for verifying compliance with and the effectiveness of these measures.

By contrast, the Department of Defense has made more progress. Specifically, the department's supply chain risk management efforts began in 2003 and include

- a policy requiring supply chain risk to be addressed early and across a system's entire life cycle and calling for an incremental implementation of supply chain risk management through a series of pilot projects;
- a requirement that every acquisition program submit and update a "program protection plan" that is to, among other things, help manage risks from supply chain exploits or design vulnerabilities;
- procedures for implementing supply chain protection measures, such as an implementation guide describing 32 specific measures for enhancing supply chain protection and procedures for program protection plans identifying ways in which programs should manage supply chain risk; and
- a monitoring mechanism to determine the status and effectiveness of supply chain protection pilot projects, as well as monitoring compliance with and effectiveness of program protection policies and procedures for several acquisition programs.

In addition, the four national security-related agencies participate in interagency efforts to address supply chain security, including participation in the Comprehensive National Cybersecurity Initiative,[12] development of technical and policy tools, and collaboration with the intelligence community. In support of the cybersecurity initiative, Defense

[12]Begun by the Bush administration in 2008, the Comprehensive National Cybersecurity Initiative is a series of initiatives aimed at improving cybersecurity within the federal government. This initiative, which is composed of 12 projects with the objective of safeguarding federal executive branch information systems, includes a project focused on addressing global supply chain risk management.

and DHS jointly lead an interagency initiative on supply chain risk management to address issues of globalization affecting the federal government's IT. Also, DHS has developed a comprehensive portfolio of technical and policy-based product offerings for federal civilian departments and agencies, including technical assessment capabilities, acquisition support, and incident response capabilities. Further, the four national security-related departments participate in an Office of the National Counterintelligence Executive-led initiative to (1) develop a common methodology for conducting threat assessments on entities that do business with the national security community and (2) request from agencies and centrally store copies of threat assessments for future use by components of the national security community.

Three National Security-Related Departments Need to Take Action to Better Address IT Supply Chain Risks

To assist the three national security-related agencies in better addressing IT supply chain-related security risks for their departmental information systems, we made several recommendations to the Secretaries of Energy and Homeland Security and the Attorney General. Specifically, we recommended that Energy

- develop and document departmental policy that defines which security measures should be employed to protect against supply chain threats;
- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

In commenting on our report, Energy stated that it concurred with the spirit of our recommendations. Energy also expressed concern that the recommendations are not fully aligned with the administration's initiatives and stated that it believes policies and standards to address IT supply chain risk management must be coordinated at the national level, not independently through individual agencies. We agree that national or federal policies and standards should be coordinated and promulgated at the national or federal level. However, we also believe–as intended by our recommendations—that federal departments are responsible for developing departmental policies and procedures that are consistent and aligned with federal guidance. Our recommendations to Energy are based

on and consistent with federal guidance on supply chain risk management.

In addition, we recommended that DHS

- develop and document departmental policy that defines which security measures should be employed to protect against supply chain threats;
- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

In commenting on a draft of our report, DHS concurred with our recommendations and described steps the department is taking to address them, including developing departmental policy to define supply chain protection measures, examining risk management procedures, and exploring options for verifying compliance with and effectiveness of its supply chain protection measures.

We also recommended that Justice

- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

Justice concurred with the recommendations.

In summary, the global IT supply chain introduces a myriad of security vulnerabilities to federal information systems that, if exploited, could introduce threats to the confidentiality, integrity, and availability of federal information systems. Thus the potential exists for serious adverse impact on an agency's operations, assets, and employees. These risks highlight the importance of national security-related agencies fully addressing supply chain security by defining measures and implementation procedures for supply chain protection and monitoring compliance with and the effectiveness of these measures. Until these agencies develop comprehensive policies, procedures, and monitoring capabilities, increased risk exists that they will be vulnerable to IT supply chain threats.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee, this completes my statement. I would be happy to answer any questions you have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen [redacted] Other key contributors to this statement include Michael W. Gilmore (Assistant Director), Bradley W. Becker, Kush K. Malhotra, and Lee McCracken.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

Mr. STEARNS. I thank you.

Mr. Komaroff, you are welcome. Opening statement.

STATEMENT OF MITCHELL KOMAROFF

Mr. KOMAROFF. Good morning, Mr. Chairman and distinguished members of the subcommittee. Thank you for this opportunity to testify regarding the efforts of the Department of Defense pertaining to supply chain risk management.

My name is Mitchell Komaroff, and I am the Director of Trusted Mission Systems and Networks within the office of the DOD Chief Information Officer. I provided a written statement for the record but would like to give you a brief overview of the globalization challenge facing the Department and to highlight——

Ms. DEGETTE. Can you move your microphone a little closer?

Mr. KOMAROFF [continuing]. To highlight key elements of our strategy for managing the risks presented by it.

The Department relies heavily on custom and commercial off-the-shelf software, integrated circuits, computers, communication equipment, and other ICT, information communications technology, to stay on the cutting edge of technology development and to fulfill mission-critical operations. With increasing frequency, the Department and its commercial supplier base rely on foreign companies to produce the most advanced technology solutions.

Although the globalization of the ICT sector has accelerated the pace of technical innovation, it has raised national security concerns. Through the increased globalization of the ICT supply chain, adversaries have more opportunities to introduce malicious code into the supply chain and to gain access or disrupt military systems. To address this challenge, DOD is implementing its trusted defense system strategy to improve the way we engineer and acquire systems and to reduce an adversary's ability to disrupt national security missions.

For years, the Department has worked to better understand and manage the risk that DOD hardware and software may contain malicious code. We were first confronted with this problem in connection with the supply of trusted application-specific integrated circuits which we addressed through the Trusted Foundry program in 2003.

The Department's strategy for achieving trustworthy systems in the face of supply chain risk contain the following core elements: one, prioritizing scarce resources based on mission criticality; two, planning for comprehensive program protection by identifying critical components and protecting them from supply chain risk informed by all-source intelligence; three, improving our ability to detect and respond to vulnerabilities in programmable logic elements; and, four, partnering with industry.

I want to briefly highlight the importance of prioritization of our strategy. The difficulty of mounting and defending against supply chain exploitation focuses supply chain risk management on sensitive mission-critical systems. Accordingly, DOD policy levies additional supply chain risk management processes and practices on national security systems.

Supply chain risk management represents a sea change in the acquisition process. It requires new institutional relationships be-

tween the acquisition and intelligence community and the application of operational security to the processes that historically we have sought to make transparent. It also requires engineering and test and evaluation capabilities that are still the subject of ongoing research.

Recognizing these challenges would take time to implement, former Deputy Secretary Lynn directed an incremental implementation of supply chain risk management beginning with pilots in fiscal years 2009 and 2010, and requiring full operational capability by fiscal year 2016 for all national security systems.

DOD is currently incorporating lessons learned during the piloting phase into permanent policy and practice. First, the Defense Intelligence Agency mission to support DOD acquisition with a supply chain threat analysis has been made permanent in DOD policy. To date, the Defense Intelligence Agency has performed approximately 520 analyses for DOD acquisition programs.

Other key tenets have been institutionalized as well, such as directing that programs integrate criticality analysis, use of supply chain threat information, supply chain risk management key practices, and hardware and software assurance into program protection.

DOD actively collaborates with industry on supply chain risk. One of our key goals is to facilitate the development of commercial global sourcing standards. DOD has been collaborating with other 20 government and industry organizations towards the development of standards under the umbrella of ISO, the International Organization for Standardization. DOD is also actively engaged in The Open Group's Trusted Technology Forum.

Within DOD, we have made a significant start to institutionalizing supply chain risk management but still have a long way to go. Our key objective for fiscal year 2012 is fully incorporating these concepts into information assurance and acquisition policies and expanding these new processes from the military departments to defense agencies. DOD has collaborated on these issues within our agency regarding proposed policies and best practices, such as the NIST interagency report and the Committee on National Security Systems Directive 505, both entitled Supply Chain Risk Management.

In conclusion, mitigating risk to U.S. Government missions arising out of the global supply chain from information and communications technology is vital to our national security. The Department looks forward to continuing the collaboration with our interagency and industry partners to manage this risk.

Thank you for the opportunity, and I look forward to answering any questions you may have.

[The prepared statement of Mr. Komaroff follows:]

STATEMENT BY

MITCHELL KOMAROFF
OFFICE OF THE DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
TRUSTED MISSION SYSTEMS & NETWORKS

BEFORE THE
HOUSE ENERGY & COMMERCE COMMITTEE
SUBCOMMITTEE ON OVERSIGHT & INVESTIGATIONS

ON

IT SUPPLY CHAIN: REVIEW OF GOVERNMENT AND INDUSTRY EFFORTS

March 27, 2012

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE ON
OVERSIGHT & INVESTIGATIONS, COMMITTEE ON ENERGY & COMMERCE

Summary

Once dominated by domestic manufacturing, today's information communications technology (ITC) manufacturing is global, and increasingly performed outside of the United States. Although the globalization of the ICT sector has accelerated the pace of technological innovation, it has also raised national security concerns that ICT hardware and software performing critical functions within its weapons and networks may contain malicious code.

In response to the forgoing globalization and supply chain risks, DoD is in the process of institutionalizing a Trusted Systems and Networks Strategy, which contains four elements: 1) Prioritize scarce resources based on mission dependence; 2) Plan for comprehensive program protection; 3) Detect and respond to vulnerabilities in programmable logic elements; and 4) Partner with industry.

The Department has undertaken an incremental approach to supply chain risk management through a series of acquisition pilot programs beginning in FY09 and FY10. DoD is now institutionalizing lessons learned during the piloting phase into permanent policy and practice. Part of DoD's strategy moving forward is to actively engage industry by participating in key standards development organizations (SDO) and reaching out at major community events, soliciting and collecting inter-agency and industry feedback, and working to develop and incorporate industry feedback into work products at the national and international levels. DoD also works with other Departments and Agencies to share lessons learned and drive best practices from piloting into USG-wide policy. Most recently, DoD and DHS worked with the Committee on National Security Systems (CNSS) to develop CNSS Directive 505 - Supply

Chain Risk Management, which serves as the supply chain policy that applies to all National Security Systems within the federal government.

Introduction

Good Morning Mr. Chairman and distinguished members of the Subcommittee. Thank you for this opportunity to testify before the Subcommittee on the Department of Defense's efforts pertaining to supply chain risk management. I am Mitchell Komaroff, and I am the Director of Trusted Mission Systems & Networks within the Office of the DoD Chief Information Officer (CIO). The Government Accountability Office (GAO) report being discussed today examines the challenge posed by insufficient security in the information technology (IT) supply chain that has the potential to lead to the exploitation of Federal networks and information. The Department of Defense (DoD) takes this challenge seriously, and is undertaking a number of steps to ensure that risks relating to the DoD's global supply chain for IT do not disrupt our ability to defend the nation. I would like to give you an overview of the challenge as it pertains to the Department and highlight our current strategy.

A. Globalization Challenge

The Department relies heavily on customized and commercial off-the-shelf (COTS) computers, communications equipment, integrated circuits (ICs), application software, and other information communications technology (ICT) to stay on the cutting edge of technology development and fulfill mission-critical operations. With increasing frequency, the Department and its commercial supplier base rely on foreign companies to produce the most advanced technology solutions. Once dominated by domestic manufacturing, globalization has caused today's ICT

manufacturing to be largely conducted outside of the United States. Globalization has led to rapid technology innovation, from which the DoD benefits greatly.

Although the globalization of the ICT sector has accelerated the pace of technological innovation, it has also raised national security concerns. Mission-critical functionality of the Department's systems and networks extensively leverages commercial, globally interconnected, and globally sourced ICT. A highly capable malicious actor can employ a full spectrum of offensive and exploitation capabilities by using a deep knowledge of latent vulnerabilities and supply chain attacks to create new vulnerabilities. As a result of this diverse global supply chain, adversaries have more opportunities to corrupt technologies, introduce malicious code into the supply chain, and otherwise gain access to the Department's military systems and networks. There is no way to return to a supplier base of "all-American" companies for the Department's ICT. Although some programs use secured facilities and cleared personnel to protect classified information when developing technology for sensitive government use, this approach is neither ideal nor financially feasible on a large scale.

B. DoD Strategy and Implementation

Background

For years, the Department has known of the risk that ICT hardware and software performing critical functions within its weapons and networks may contain malicious code and has been working to address this risk. By 2003, DoD could no longer afford to internally produce leading edge application specific integrated circuits (ASICs), and so established the Trusted Foundry program to ensure trusted, leading edge military unique chips could be acquired from commercial industry. In the 2004-2006 timeframe, DoD CIO and the Under Secretary of

Defense for Acquisition, Technology and Logistics (USD(AT&L)) considered similar issues associated with software within their Software Assurance Tiger Team effort. This effort elevated the software/hardware issues to the systems-level, and formulated a full lifecycle strategy involving system prioritization, identification and protection of critical system functions and ICT components, use of all source intelligence to understand supply chain risk, enhanced test and evaluation for vulnerability detection, and industry engagement. These strategy elements and the key partnership between information assurance and acquisition continue to animate DoD policy and implementation as described below.

Trusted Systems and Networks Strategy

In response to the forgoing globalization and supply chain risks, DoD is in the process of institutionalizing the Trusted Defense Systems / Supply Chain Risk Management (SCRM) strategies described in the Report on Trusted Defense Systems in response to the FY09 National Defense Authorization Act (NDAA), Section 254, delivered to the Congress in January 2010. The Department's strategy for achieving trustworthy defense information and weapons systems in light of supply chain risk contains the following core elements:

1. **Prioritize scarce resources based on mission dependence** – Allocate the Department's systems assurance resources based on a system's criticality and risk of attack. The difficulty of mounting and defending against supply chain attacks focuses supply chain risk management on sensitive, mission critical systems. Accordingly, DoD policy levies the requirement of trusted systems / supply chain risk processes and practices only on National Security Systems (NSS).

2. **Plan for comprehensive program protection** – Employ comprehensive program protection planning, including systems engineering, supply chain risk management key practices, hardware and software assurance, counterintelligence, test and evaluation and information assurance to identify and protect critical components, functions, technologies, and information using a full range of tools, resources, and practices. Our strategy is focused on making these tools, resources, and practices available to protect the most critical functions and components of NSS. DoD requires acquisition programs to perform criticality analysis, by which they identify mission-critical functions and components, down to the commercial hardware, software, and firmware components that implement those functions. The critical components so identified become the focus of protection activities, including use of all source threat analysis to identify supply chain risk, and enhanced test and evaluation.

3. **Detect and respond to vulnerabilities in programmable logic elements** – Invest in enhanced vulnerability detection research and development, and transition such analytical capabilities to support acquisition.

4. **Partner with industry** – Collaborate with industry to develop commercially reasonable standards for global sourcing and SCRM and to identify leading edge commercial practices and tools.

Incremental Implementation

Supply Chain Risk Management (SCRM) represents a change in the acquisition process. It requires new institutional relationships between acquisition and the intelligence community, and

application of operations security to processes that have historically sought to be transparent. Beginning with the Comprehensive National Cyber Security Initiative (CNCI) Initiative 11 in 2008, co-led by DoD and the Department of Homeland Security (DHS), the DoD strategy has been incremental implementation of the new processes and practices through pilots. DoD Directive Type Memorandum (DTM) 08-048, February 19, 2009, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems" provided the framework for DoD implementation of SCRM.

In DTM 08-048 (reissued March 25, 2010, 09-016), DoD Deputy Secretary Lynn directed incremental implementation of SCRM as outlined in the above strategy beginning with pilots in FY09/10 and requiring full operational capability by FY16 for all NSS. The DTM also established the mission at the Defense Intelligence Agency (DIA) to provide supply chain threat analyses to DoD acquisition programs, and directed vulnerability assessments to meet the requirements of FY09 NDAA Section 254.

The key objectives in FY09/10 were:

1) Establishing institutional relationships between Military Department (MILDEP) acquisition programs (through then "SCRM Centers of Excellence" now "SCRM Focal Points") and the new DIA Threat Analysis Center (TAC) threat assessment capability;

2) Developing, evaluating, and documenting SCRM best practices in the DoD SCRM Key Practices Guide; and

3) Performing FY09 NDAA Section 254 Congressional direction.

During this period, DoD performed "Center of Excellence" pilots and vulnerability assessments under FY09 NDAA Section 254, during which acquisition programs leveraged DIA TAC analysis, and assessed practices within the DoD SCRM Key Practices Guide. These activities validated DoD strategies, confirmed that SCRM was necessary to manage risk being assumed by DoD programs, and exercised new DIA TAC intelligence capabilities. FY09/10 pilots were documented in the Section 254 "Trusted Defense Systems" Report to Congress in December of 2009, and "CNCI DoD Supply Chain Risk Management (SCRM) Pilot Program Report" in April of 2011. During this period, based upon lessons learned, DoD engaged with its oversight committees to seek clarification to use new intelligence capabilities within its procurement processes, leading to FY11 NDAA Section 806, "Requirements for Information Relating to Supply Chain Risk."

DoD is currently institutionalizing lessons learned during the piloting phase into permanent policy and practice.

- First, the DIA mission to support DoD acquisition with supply chain threat analysis has been made permanent in DoD Instruction (DoDI) 5240.24, June 8, 2011, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)." To date, DIA TAC has performed approximately 520 analyses for DoD acquisition programs.

- Other key tenets were institutionalized on July 18, 2011, when the Principal Deputy USD(AT&L) issued a Memorandum to all DoD Component Acquisition Executives directing that Program Protection Plans (PPP) incorporate key elements of the above Trusted Defense System/SCRM Strategy, including criticality analysis, use of DIA TAC

analyses, SCRM Key Practices, and hardware and software assurance. To help institutionalize the prioritization process, DoD developed a rigorous Criticality Analysis methodology and has engaged over 60 programs to implement it. In addition, over 25 major system acquisitions have incorporated SCRM into their PPPs.

- We will further institutionalize the concepts we piloted through the DoDI 5200.MM, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks." That instruction, in the final stages of coordination, will be signed out by the DoD CIO and the USD(AT&L), and will make the Trusted Defense Systems/SCRM Strategy outlined above and issued in the DTM 08-048 permanent. It requires that risks to critical functions and components of mission-critical systems be protected across the entire system lifecycle, and is the policy that will enable full operating capability for SCRM across the Department. DoDI 5200.MM applies SCRM practices piloted within the MILDEPS across the entire Department. DoD is in the process of establishing SCRM Focal Points in each of the Defense Agencies.

- Lastly, we are working to fully implement FY11 NDAA Section 806, which clarifies DoD authority to use intelligence within its procurement processes. The statute sets forth procedures that enable DoD under specified circumstances to exclude a particular source who presents an unacceptable level of supply chain risk, and withhold certain information regarding the basis of that decision. DoD is working through a series of tabletop exercises and pilots to determine the best way to integrate the authority into its processes.

Although DoD has begun to institutionalize the strategies and lessons learned of from its earlier studies and FY09/10 pilot activities, it is very early in the journey toward full operational capability as required by Policy. Its current procedures will ensure that supply chain risk will be identified. However, many of the techniques for mitigating risk are difficult for programs to implement, and some are the subject of active research and development.

C. Partnership with Industry

DoD engages in a robust collaboration with industry to collect, analyze and share SCRM best practices and to better understand the level of risk the USG accepts when procuring ICT from commercial suppliers and integrators. DoD's strategy is to actively engage industry by participating in key standards development organizations (SDO) and reaching out at major community events, soliciting and collecting inter-agency and industry feedback, and working to develop and incorporate industry feedback into work products at the national and international levels. Additionally, DoD collaborates along with the National Institute for Standards and Technology (NIST) in the DHS-led Software Assurance (SwA) Program. The SwA Program hosts quarterly Forums & Working Groups to bring together members of government, industry, and academia with vested interests in software assurance to discuss and promote integrity, security, and reliability in software, in the supply chain.

One of the key standardization and outreach goals is to facilitate development and adoption of commercial global sourcing standards, which will enable DoD and other USG acquirers of ICT products and services to better communicate in ICT requirements, and to establish industry practices for validating those requirements have been satisfied. To achieve this goal, DoD is engaged in several key national and international standardization efforts, including the

International Organization for Standardization (ISO) and other key SDOs. In addition, the Department partners with over 20 government and industry organizations as well as the Information Security Forum (ISF), a global non-profit with 300 corporation members, towards the development of commercially-reasonable standards for global sourcing.

DoD is also engaged in The Open Group's "Trusted Technology Forum" (OTTF). The OTTF strives to provide a collaborative, open environment for technology companies, customers, government, and supplier organizations to create and promote guidelines for manufacturing, sourcing, and integrating trusted, secure technologies, shape global procurement strategies and best practices to help reduce threats and vulnerabilities in the global supply chain. OTTF recently released a "snapshot" of their "trusted technology provider framework" (TTPF) which documents best practices against counterfeits and tainted products. DoD is working with OTTF to foster standards harmonization with the existing "mutual recognition" Common Criteria for product evaluations and other related ISO / international standards.

These are just a few of the venues where DoD collaborates with a variety of other government, industry, and public/private activities to solve the ICT SCRM challenge. In the next 3 years, DoD strives to move these various efforts forward with the goal of having a family of related ICT SCRM standards available for USG and industry to use for establishing mature relationships with ICT service and product providers. The ultimate goal of the standardization efforts is to help raise the bar of best practice globally to help create a more transparent environment for acquirers of ICT services and products.

D. Way Ahead

DoD continues to march towards full scale implementation of DoD's SCRM Program while participating in CNCI and partnering with the Committee for National Security Systems (CNSS) and other agencies to advance SCRM efforts across mission critical USG systems and networks. Within DoD, a key objective for 2012 is developing an integrated set of information assurance and acquisition policies to reflect SCRM concepts. DoD CIO and USD(AT&L) will continue to support the Military Services and Defense Agencies as they build out their capabilities and will provide guidance and support to programs on how to identify and manage risk they may have already accepted. Training, education, and awareness efforts will be an important part of these efforts going forward.

Since its efforts in CNCI Initiative 11, DoD has collaborated with the Interagency regarding proposed policies, processes and SCRM best practices. The DoD SCRM Key Practices were shared with DHS and NIST at an early point, and have been made available to the larger community as the NIST Interagency Report 7622, "Supply Chain Risk Management." In the area of Policy, DoD Directive Type Memorandum 09-016, "Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems" and its draft Instruction 5200.MM, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks" have been shared with the Interagency, and through the Committee on National Security systems (CNSS) Directive 505, "Supply Chain Risk Management" has been made binding on all USG National Security systems.

CNSS Directive 505, "Supply Chain Risk Management" adopts concepts, lessons learned and strategy elements from the DoD's SCRM strategy and issuances, including elements of the incremental approach to implementing SCRM. Within the first year of 505's issuance, agencies are to develop an initial SCRM capability, and within six years of the issuance's publication, agencies are to have developed a full-scale SCRM capability to protect their NSS. This model has been successful in the DoD, and through lessons learned has set the stage for a successful implementation by interagency.

Conclusion

Mitigating risks to the Department's missions from the global supply chain for ICT is critical to our national security. The efforts that I have outlined today detail what the Department has done and is planning to continue to do to ensure effective supply chain risk management. I want to thank you for your interest in our efforts and I am happy to answer any questions you may have.

Mr. STEARNS. Thank you very much.
Mr. VEGA.

STATEMENT OF GIL VEGA

Mr. VEGA. Good morning, Chairman Stearns, Ranking Member DeGette, and members of the subcommittee. My name is Gil Vega, and I am the Associate Chief Information Officer for Cybersecurity at the Department of Energy. I also serve as the Department's Chief Information Security Officer. Thank you for this opportunity to testify today on the GAO report that is the subject of today's hearing.

The Department of Energy appreciates the work performed by the GAO to identify opportunities to improve mission effectiveness by reducing IT supply chain risks. DOE shares GAO's concerns for these risks, which not only impact our missions but those of all Federal agencies and the private sector.

DOE actively supports the goals outlined in the administration's recently released National Strategy for Global Supply Chain Security, and by leveraging the exceptional talent of the people in DOE we are committed to addressing these challenges.

It is clear that supply chain, including IT supply chain, vulnerabilities threaten the missions of DOE and other agencies. As the Department's Chief Information Security Officer, I am briefed daily on the active and persistent nature of threats directed at DOE. One of my primary roles is to evaluate these threats to our unique full-spectrum mission from open science to energy research, to nuclear security, and establish effective agency-wide programs to mitigate the associated risks in a cost-effective manner.

In my short time at DOE, I have been privileged to work with cybersecurity leaders in our National Laboratories and with interagencypartners who are committed to addressing this national-level challenge by partnering and sharing information and best practices with each other. Aligned with the Secretary's goals related to energy, economic, and national security, we are leveraging the expertise of our National Laboratories to develop processes and technology to effectively secure DOE's IT assets and to protect the Nation's critical infrastructure.

To address cybersecurity threats, you must first build sound foundational components and by recognizing that no single organization can eliminate all risk. Recently, DOE has been successful in developing and delivering several key foundational elements to properly address the broader cybersecurity threats that we face while strengthening our ability to meet the wide range of mission goals.

For example, DOE has developed and is implementing an agency-wide NIST-based risk management approach that raises corporate threat analysis and risk decision-making to senior management levels of DOE and serves as a corporate foundation for managing our mission and investments with acceptable levels of risk.

DOE is also implementing the Joint Cybersecurity Coordination Center, which is delivering a new cybersecurity ecosystem based on consolidated monitoring and reporting, information sharing and analysis, and coordinated incident response capabilities across the

Department. This is critical to the effective monitoring of mitigation strategies meant to address advanced cyber threats.

As I previously stated, DOE recognizes the value and timing of the GAO review and concurs with GAO's recommendations. Specifically, we are already addressing these in a coordinated manner as follows: by actively participating in the national-level policy discussions on supply chain risk management; by developing a supply chain cybersecurity strategy and policy that will foster DOE's interagency relationships and support the unified approach described in the administration's strategy; by developing a plan to implement the requirements of the recently released Committee on National Security Systems Directive 505; by working closely with the National Counterintelligence Executive and the broader national intelligence and national security communities to stay abreast of and counter new and growing threats to the Nation's IT infrastructure; and, finally, by partnering with both DHS and DOD, industrial control system manufacturers, and energy-critical infrastructure operators to identify and mitigate risks to industrial control systems.

We must also recognize the importance of the role played by DOE's National Laboratories, which have been at the forefront of identifying and mitigating vulnerabilities in the supply chain. DOE's National Laboratories have developed and are actively involved in improving capabilities in software and hardware assurance to mitigate risks, particularly to our national security systems and to the safety, security, and reliability of the Nation's nuclear weapons stockpile. DOE works closely with other agencies on these emerging capabilities.

In conclusion, we believe that GAO understands the national challenge that IT supply chain risks pose to all Federal agencies as well as to the private sector and believe further congressional support for a nationally coordinated response is required.

Again, DOE strongly supports the goals of the President's strategy, which seeks to align Federal activities across the United States Government, including in our partnerships with industry. DOE believes that this unified approach is the right approach and that policies and standards to address IT supply chain risk management must be coordinated at the national level.

Thank you for this opportunity to discuss the report's findings.

Mr. Chairman, this concludes my statement, and I look forward to answering all of your questions.

[The prepared statement of Mr. Vega follows:]

Statement of Gil Vega

Associate Chief Information Officer for Cybersecurity and Chief Information Security Officer

U.S. Department of Energy

Before the

Subcommittee on Oversight and Investigations

Committee on Energy and Commerce

U.S. House of Representatives

March 27, 2012

Good morning Mr. Chairman Stearns and Members of the Subcommittee. I am pleased to testify on the Department of Energy's activities related to IT supply chain security. Thank you for this opportunity to testify today on the Government Accountability Office's (GAO) report titled *IT Supply Chain- National Security Related Agencies Need to Better Address Risk*s. The Department of Energy (DOE) appreciates the work performed by the GAO to identify opportunities to improve mission effectiveness and fiscal efficiency by reducing information technology (IT) supply chain risks. The DOE shares GAO's concern for these risks, which not only impact DOE's missions, but those of all federal agencies and the private sector in general. The DOE actively supports the goals outlined in the Administration's *National Strategy for Global Supply Chain Security* (January 2012) and by leveraging the collective, exceptional talent

of the people in the DOE, we are committed to addressing these and other cybersecurity challenges.

Background

In November 2010, the GAO began a multi-agency review to identify efforts the Departments of Defense (DoD), Homeland Security (DHS), Justice (DOJ) and Energy (DOE) were taking to address IT supply chain risks. In response to its conclusions that agencies needed to better address supply chain risks, GAO's report directed three recommendations to DOE:

- Develop and document Departmental policy that defines which security measures should be employed to protect against supply chain threats;
- Develop, document and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- Develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain measures.

Department of Energy Response

It is clear that IT supply chain vulnerabilities threaten the missions of DOE and other federal agencies. As the Associate Chief Information Officer for Cybersecurity and the DOE Chief Information Security Officer, one of my roles is to understand and evaluate the cybersecurity threats to our missions and establish effective agency-wide programs to mitigate the associated risks in a cost-effective manner. Throughout my career, I have led similar efforts to effectively, and cost-efficiently, manage security risk.

In my short time at the DOE, I have been privileged to work with cybersecurity thought leaders in our National Laboratories and with interagency partners who are committed to addressing this national-level challenge by partnering and sharing information and best practices with each other, academia and industry. Aligned with the DOE Secretary's goals related to energy, economic and national security, we are leveraging the experience and expertise of our National Laboratories to develop processes and technology to effectively secure DOE's IT assets and information, and to protect the nation's critical infrastructure.

Over the past 12 months, the DOE has been successful in developing and delivering several key foundational elements to properly address the broader cybersecurity threats we face every day, while strengthening our ability to meet the wide range of mission goals, which span open science to nuclear security. Among these accomplishments:

- DOE has developed and is implementing an agency-wide NIST-based Risk Management Approach with strategic direction and oversight by an Undersecretary-level Information Management Governance Council (IMGC). This raises corporate threat analysis and risk decision-making to senior management levels of the DOE and serves as a corporate foundation for managing our mission and investments with acceptable levels of risk. This is critical to the success and return on investment of current and future IT supply chain risk mitigation strategies.
- Under the direction and leadership of the IMGC, DOE is implementing an agency-wide Joint Cybersecurity Coordination Center, which will create a new cyber operational ecosystem with consolidated monitoring and reporting, collaborative information sharing and analysis, and coordinated incident response capabilities across the DOE. This is

critical to the effective monitoring of mitigation strategies implemented to address advanced cyber threats in general, and IT supply chain risks specifically.

As I previously stated, the DOE concurs with the GAO's recommendations. We are already addressing these in a coordinated manner by:

- Actively participating in the national-level policy discussions on Supply Chain Risk Management;
- Developing a supply chain cybersecurity strategy and policy that will foster DOE's interagency relationships and support the unified approach described in the Administration's *National Strategy For Global Supply Chain Security*;
- Developing a plan to implement the requirements of the recently released Committee on National Security Systems Directive 505, *Supply Chain Risk Management Directive for National Security Systems*;
- Working closely with the National Counterintelligence Executive and the broader National Intelligence and National Security communities to stay abreast of and counter new and growing threats to the nation's IT infrastructure; and
- Partnering with DHS and DoD, industrial control system manufacturers and energy critical infrastructure operators to identify and mitigate risks to industrial control systems.

While securing the supply chain will require more than any one agency can accomplish on its own, it is important to recognize the importance of the role played by DOE's National Laboratories, which have been at the forefront of identifying and mitigating vulnerabilities in the IT supply chain. The DOE National Laboratories have developed and are actively improving capabilities in software and hardware assurance to mitigate risks, particularly to our National

Security Systems and to the safety, security and reliability of the nuclear weapons stockpile. The DOE works closely with DoD, DHS, the National Security Agency, the Department of Commerce, and the General Services Administration on these emerging capabilities.

Conclusion

In conclusion, the GAO report has identified areas of needed improvement for IT supply chain security at the DOE and we concur with the report's recommendations. We believe GAO understands the national challenge IT supply chain risks pose to all federal agencies as well as the private sector and believe further congressional support for a nationally coordinated response is required.

The DOE strongly supports the goals of the *National Strategy for Global Supply Chain Security*, which address the need to "promote the secure and efficient movement of goods" and to "foster a resilient supply chain". To this end, the Administration has communicated that it seeks to align Federal activities across the United States Government, including in our partnerships with industry. The DOE believes that this unified approach is the right approach, and that policies and standards to address IT supply chain risk management must be coordinated at the national level, not developed independently through individual agencies.

Meanwhile, at DOE, we understand how important our role is as the sector-specific agency, as designated under Homeland Security Presidential Directive-7, for the nation's energy critical infrastructure and as a cornerstone of our nuclear security. We will continue our efforts to strengthen cybersecurity in these specific programs, as well as across the entire DOE enterprise.

Thank you for this opportunity to discuss the report's findings. Mr. Chairman, this concludes my statement and I look forward to answering your questions.

Mr. STEARNS. Thank you, Mr. Vega.

Let me just open up with just sort of a general statement when we are talking about IT supply chain. And this is a question for each of you. Would you think that the biggest emerging threat to the government and consumers is this IT supply chain? Just yes or no.

Mr. WILSHUSEN. No.

Mr. STEARNS. No, OK.

Mr. Komaroff? Yes or no?

Mr. KOMAROFF. For some systems, yes.

Mr. STEARNS. Mr. Vega?

Mr. VEGA. I would say no.

Mr. STEARNS. No, OK.

And when you talk about supply chain, I just want to define it. Are we talking about smartphones, computers, TPS devices, smart grid devices? Have I missed out anyone of the list I gave you?

Mr. WILSHUSEN. It could be any—the whole—the whole slew.

Mr. STEARNS. A panoply of many devices.

Mr. WILSHUSEN. So there are additional types of devices and components of those devices, to include servers——

Mr. STEARNS. Of the four I mentioned, you think there could be more.

Mr. WILSHUSEN. Yes.

Mr. STEARNS. OK, and—I am just trying to get a general, what we are talking about, if I can.

Mr. KOMAROFF. Yes, sir. So——

Mr. STEARNS. More than those four devices we could be looking at.

Mr. KOMAROFF. Yes, there is a huge number.

Mr. STEARNS. OK, huge number. Can you give me maybe an ancillary one that we haven't thought about?

Mr. KOMAROFF. Well, there are just dozens, and dozens of varieties of integrated circuits that——

Mr. STEARNS. Oh, OK.

Mr. KOMAROFF [continuing]. Some systems integrators go out into the commercial marketplace to acquire.

Mr. STEARNS. OK, Mr. Vega?

Mr. VEGA. I am not sure if I heard you say, but the underlying telecommunications infrastructure is another one that we are concerned about.

Mr. STEARNS. OK. Mr. Wilshusen, this question is for you. You have identified risk to unprotected systems including malicious code on hardware and software, counterfeit hardware or software, reliance upon malicious or unqualified service provider. What do you see as the two greatest threats to our IT supply chain?

Mr. WILSHUSEN. I would say first, one would be the introduction or insertion of malicious code to hardware and software and also, presently, counterfeits. Counterfeit items have been on the increase, and certainly they can have a debilitating effect on systems that are currently in operation.

Mr. STEARNS. Can you give the committee a list of specific examples?

Mr. WILSHUSEN. Sure.

Mr. STEARNS. Examples of threats, I mean.

Mr. WILSHUSEN. Well, threats and also incidents, if you will. You know, there is—back in 2010, the Department of Commerce issued a report that identified, did a survey of companies that participated in the DIB, Defense Industrial Base; and of the 387 companies that participated in the survey, 39 percent of them encountered counterfeit electronics during a 4-year period. And what's more, the number of incidents of those counterfeit items increased 140 percent over the 4-year period, from about 3,800 items in 2005 to over 9,000 in 2008.

Mr. STEARNS. All right. Mr. Komaroff, yesterday the GAO released a different report on counterfeit military parts manufactured overseas showing the prevalence of counterfeit parts in the DOD's Internet purchasing system. Has the work you have done led to a similar conclusion?

Mr. KOMAROFF. Yes, sir. So I don't want to speak to the exact conclusions contained in that report, but within the report that we submitted to the Congress in 2010 in response to the 2009 Defense Authorization Act, the report entitled Trusted Defense Systems where we outlined our strategy, we did identify, you know, risks during the sustainment and, in particular, counterfeits as a strategic gap in our strategies. And since that time immediately began working it within the Department and then more recently in collaboration with the intellectual property coordinator. And policy has been issued within the Department identifying the Assistant Secretary for Supply Chain Integration as the lead for the Department on counterfeit issues, and the Department is pressing forward to work those issues.

Mr. STEARNS. What is the common specific threat to DOD supply chain that you have identified?

Mr. KOMAROFF. The common threat, sir?

Mr. STEARNS. What is the most common threat to the Department of Defense's supply chain?

Mr. KOMAROFF. The most common occurring threat, presumably, would be in the realm of the counterfeit issue because of its prevalence. Again, that is a different—typically, a different sort of threat actor and is more of a threat to the effectiveness of reliability engineering than the kind of threat that would be presented, for instance, with a—you know, an attempt by a foreign intelligence service to insinuate itself into a national security system of great importance.

Mr. STEARNS. Mr. Vega, can you specifically give me actual cyber attacks or threats to the Department of Energy's systems because of vulnerability? Can you give any specific examples?

Mr. VEGA. If I could——

Mr. STEARNS. Or are you aware of any cybersecurity threats, attacks to the Department of Energy? You don't have to get into detail, but, I mean, are you aware of any specific threats?

Mr. VEGA. Absolutely, and I would say, Chairman, that our number one concern at the Department of Energy are the coordinated efforts by some adversaries whose capabilities in the arena of computer hacking are world class. We have all read about these advanced persistent threats. We have had experience at the Department of Energy with incidents involving these threat actors, and that continues to be a major area of concern for us.

Mr. STEARNS. All right, my time is expired. The gentlelady from Colorado.

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

I am glad to see again Mr. Wilshusen. When you were last here, you talked about cybersecurity risks for the electric grid, and we talked then about the risk of cyber attacks on the electric grid supply chain. So now I am happy to have you back to talk about the threats and vulnerabilities in the IT supply chains.

What are the key IT supply chain threats to Federal agencies?

Mr. WILSHUSEN. Well, we would say that it would include the insertion of malicious or harmful software and hardware into the environment. The installation of counterfeit items certainly would be key to that and also any potential disruption in the production or distribution of these key items. Certainly, that would also have a role in the key threat.

And also I would finally say, too, in terms of the installation of software, hardware that contains unintentional vulnerabilities, and these would be, for example, like design flaws in the equipment or software defects and coding defects into the software.

Ms. DEGETTE. That could be taking advantage.

Mr. WILSHUSEN. Yes. And indeed we often find that such defects are indeed taken advantage of once the software is in fact placed into operation at agencies.

Ms. DEGETTE. And do you think most of the threats come through commercial items that are purchased by the Federal Government?

Mr. WILSHUSEN. Yes, in some form or manner.

Ms. DEGETTE. So why then are the Federal agencies relying so heavily on these commercial components? Are there incentives in place for them to purchase these commercial items versus developing IT products in-house?

Mr. WILSHUSEN. Certainly. And I think it is the administration's policy to take full advantage of those commercial off-the-self products, both from cost savings as well as the functionality that they provide. It always gets back to kind of a risk management decision on whether or not we should use commercial products or potentially develop inside.

Ms. DEGETTE. And, in fact, there is an OMB circular that encourages agencies to purchase the off-the-shelf items wherever possible, is that correct?

Mr. WILSHUSEN. That's correct.

Ms. DEGETTE. Mr. Komaroff, you are nodding your head yes, too.

Mr. KOMAROFF. As I understand the matter, it has been a long-term Federal policy for so many years.

Ms. DEGETTE. It is not just new under this administration.

Mr. KOMAROFF. That's correct.

Ms. DEGETTE. It has been in place for a long time.

And even independent of the statutory incentives, is it even conceivable that Federal Government agencies would rely on non-commercial IT components for the majority of the source, Mr. Wilshusen?

Mr. WILSHUSEN. For the majority of its equipment?

Ms. DEGETTE. Right.

Mr. WILSHUSEN. Probably not, but there certainly would be instances, they may want to do something in a trusted environment in terms of developing a system or components of systems, particularly for those that have a great deal of sensitivity and criticality to potential——

Ms. DEGETTE. So we are talking today about addressing the IT supply chain threats, and that is important, but we shouldn't forget that these threats impact more than the Department of Defense and the Department of Energy. It is fair to say, isn't it, Mr. Wilshusen, that the threat you just described can also impact private-sector commercial purchasers of IT products, correct?

Mr. WILSHUSEN. Absolutely.

Ms. DEGETTE. And the issue of commercial impact is important, too, because much of our critical infrastructure, like the electric grid, for example, is run by private companies, and that is a network of private and public. So as the systems become more interoperable the repercussions of one single flawed component piece becomes more powerful, is that right?

Mr. WILSHUSEN. I would agree.

Ms. DEGETTE. So not all companies have the ability to closely vet IT supply chain threats to the product components they purchase, do they?

Mr. WILSHUSEN. No.

Ms. DEGETTE. And let me just give you an example. If there is a small business who is a contractor and they have one or two employees, they might not be able to make sure that the software they purchase isn't counterfeit or hasn't been infected with some kind of malware, is that right?

Mr. WILSHUSEN. That is very likely.

Ms. DEGETTE. So can you give us some advice about what the right balance is here? You know, the Federal Government can't always ensure the security of every single purchase by even every single one of their contractors or their subcontractors. So what is the best way for us to use Federal resources to try to, as best we can, achieve the goal of a secure supply chain?

Mr. WILSHUSEN. Well, I think there are a couple of things. First of all, the Federal agencies and under the Comprehensive National Cybersecurity Initiative, which is led by DHS and DOD, and they have developed a working group to look at different activities, threat assessment tools, and other best practices that could potentially be used to assess and to try to mitigate the risk associated with supply chain. And certainly, to the extent—I should say a key focus of that initiative is to partner with the private sector. And certainly the private sector is a key part of the whole IT supply chain. And working with the private sector and using some of the tools developed by these agencies could be of benefit to others.

Ms. DEGETTE. Thank you very much.

Thank you, Mr. Chairman.

Mr. STEARNS. Mrs. Myrick is recognized for 5 minutes.

Mrs. MYRICK. Thank you, Mr. Chairman.

I appreciate you all being here, and I appreciate your GAO report. It is an issue I have been spending a lot of time on lately. I am especially concerned about foreign, state-owned governments and militaries who are providing equipment, trying to get a foot-

hold into this area. China is the main one that I have spent time on.

And my concern is twofold. One, of course, with our government agencies, and I agree that the working groups are doing a much better job of trying to look over the whole spectrum of what is needed within the government.

But going back to the question of the private sector and how we relate, because a lot of what we buy we buy from the private sector as well, and they maybe don't know that they are either buying a piece of equipment or a router or something that is not good. Do we—I know we work with them, but how are we looking at, across the industry, is there anything else that you think we can do relative to putting more certainty into the fact that they know what they are doing and what they are providing to us?

That is one question.

Mr. WILSHUSEN. OK, I would say certainly, you know, with the interagency working groups that are looking at this, and indeed the administration just came out in January with its National Strategy for Global Supply Chain Security, and one of the focuses of that particular strategy is to work with the private sector and State and local governments as well——

Mrs. MYRICK. Right.

Mr. WILSHUSEN [continuing]. And other stakeholders to look across the entire spectrum in looking at the threats, the vulnerabilities, getting a better awareness of those, and then to work collaboratively and develop the tools and techniques try to mitigate that. So that certainly is a goal of this strategy.

One of the things that we noted in looking at this strategy, however, is that it seems to focus on the movement of goods and services from point A to point B——

Mrs. MYRICK. Right.

Mr. WILSHUSEN. —to point C and not really address the manufacture or the assembly and integration of those products and components into supply—or into full systems. And that's something that should probably be—something that we just notice in looking at it.

Mrs. MYRICK. Well, part of that also is price. Because everybody is looking at price today, and they want to buy cheap. And the foreign governments or the foreign militaries or the people who are part of these companies are literally dropping their price so low that our companies can't compete with them, and so people will buy it just because it is cheaper. And we see that over and over and over again. And it is very frightening to me, because we are at such high risk from the things that they can do to us.

And so, you know, I just encourage all of you, I know you do it every day, but anything that you can do, you know, to look at this and your supply chain of what you buy and how you work with the private sector to help them, I would sure appreciate. Because it is not going to get better. It is going to get worse. The ways that they are trying to get equipment into here are frightening to me.

So I yield back, Mr. Chairman.

Mr. STEARNS. Mr. Scalise is recognized for 5 minutes.

Mr. SCALISE. Thank you, Mr. Chairman. I appreciate you having this, and I appreciate the panelists who are here with us on the GAO report on supply chain.

I apologize if this was already brought up. Mr. Vega, on the Department of Energy, there were some issues that they had brought up. I think they—you know, on DOD, they had a pretty good assessment there, but on DOE they had raised some issues. And, you know, especially when you look at some of the sensitive nature of some of the things that the Department of Energy has and, of course, management of our nuclear weapons stockpile, among other things. If you could just kind of give me your take on the issues that were brought up in that GAO report.

Mr. VEGA. Sure. I thank you for the question.

I think the report brings up some very good recommendations, and I think there is some room at the Department of Energy to be more explicit about the policy relating to supply chain risk management and also about the processes and also the controls to the systems to monitor the implementation of those processes.

But I will tell you that the Department of Energy is very active in delivering some very foundational elements that are associated with detecting, mitigating, and responding to many different types of threats targeted at the Department of Energy. We have many threats that we are concerned about. Supply chain risk management is certainly one of those. You heard me talk about the organized attackers that target government agencies. There is also trusted insiders that we are focused on detecting and responding to, a whole litany of different threats are pointed at not only to the Department of Energy but other Cabinet agencies as well.

Our focus on supply chain, however, is in the broader sense related to the risk-management approach that the Department of Energy is embarking upon. Recently, in the past year, the Department of Energy has implemented this new risk-management approach which is mission-focused and allows—and directs those business owners to direct limited resources at the things that are most important to the mission and the most sensitive—the most sensitive data.

My office has issued architectural frameworks that actually direct these business and system owners to account for supply chain risk management as part of their overall risk-assessment process.

Mr. SCALISE. In the last year, have you all had any reported incidents—and I open this up to everybody—you know, what kinds of things that have happened and, you know, have you—we hear in the private sector all the time a lot of high-profile examples of systems that were violated, breaches that occurred; and, in some cases, we have identified back to specific countries where this is happening, you know.

Have you had any of those experiences as you encounter some of the things that are happening, in some cases possibly government-led, by foreign governments? Do you all talk to the State Department, you know, to try to get—to get some of those problems addressed at the State level where we know there's some foreign countries that are trying to break into our systems, both government and private sector?

Mr. VEGA. Without getting into too many specifics, the Department of Energy has experienced recent events that have been widely publicized in the past year at some of our National Laboratories. Without speaking directly to the nation-state implications of those events, I will tell you that the Department of Energy is engaged at the interagency level with the White House on a government-wide response to these advanced threats, and I would be more than happy to talk to you more in a closed session about what some of those discussions entail.

Mr. SCALISE. Sure. Mr. Komaroff?

Mr. KOMAROFF. I would defer, you know, to others on the broad spectrum of cyber-related exploitation that could be affecting the Department's systems and networks. I think that that shades into the presence of counterfeits and components and what have you that have been identified within the Department. I don't think that there is strong enough evidence to present a no-kidding instance of what I would call a true supply chain exploitation accounting for any one of them.

Malicious code account—malicious code, so-called, accounts for, which is generally code injected into systems, typically remotely, frequently exploits the kinds of weaknesses and security defects in devices that we acquire. That is kind of a different problem and is the basics of information assurance and cybersecurity.

Supply chain risk, as we address it, represents a much smaller set and much more difficult to discern. There will be instances where we put two and two together, see a threat actor, and examine equipment and find weaknesses associated with it. Those weaknesses frequently could be explained as either security related defects or the failure to close engineering-type back doors and what have you.

Ultimately, it is a subtle matter trying to discern whether or not a particular instance is the case of an explicable—an otherwise explicable defect or a no-kidding supply chain exploitation.

Mr. SCALISE. I see my time is up.

Mr. STEARNS. I appreciate it.

The gentleman from Texas, Mr. Green, is recognized for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

American manufacturers rely heavily on the global supply chain to build products and hardware, for the devices can be made and assembled in any country in the world. Software code can be written everywhere. This means that foreign governments can have access to these components at several entry points, and these components can make their way into any number of places via government entities or private-sector uses through critical infrastructure components and controls and even through personal electronics.

Mr. Wilshusen, are most IT product components manufactured in the U.S.?

Mr. WILSHUSEN. I would say no.

Mr. GREEN. Do you know where a lot of these components are manufactured?

Mr. WILSHUSEN. It could be anywhere—anywhere on the planet, generally.

In the report we just issued, we have a diagram of a laptop, and from that we identified various different components of your basic laptop like the LCD, the motherboard, circuits, memoryS storage and hard drives, and each of those products could come from any number of multiple different countries, except for the motherboard. I think we only found that coming from Taiwan, but——

Mr. GREEN. Oftentimes, the purchaser of the ultimate product isn't aware of where all the components are from. Because, again, even an individual, if you buy your cell phone or your—you know, BlackBerry or whatever. So a government entity could purchase a product from an American brand and not be—and be unaware of where all the component pieces in it were manufactured or assembled.

Mr. WILSHUSEN. Yes, I would say definitely so.

Mr. GREEN. This leaves government purchases heavily exposed, and right now companies are not obligated to inform the government in commercial or individual purchases of where the products they sell come from.

Mr. Wilshusen, do government entities currently track where all of their components come from?

Mr. WILSHUSEN. No, they don't. And particularly one of the objectives that we had in our report that we issued dealt with the extent to which the four agencies that we went to—Energy, Homeland Security, Justice, and DOD—on the extent to which they tracked the foreign location of these components, and none of them actually tracked those.

But then again they weren't required to track it either, and there is a thought that trying to do so would be cost-prohibitive and that perhaps a more indicative—or an indication of the threat and risk would be not so much location of a facility where a component is prepared but more it is the influence that an either foreign intelligence service or some other organization may have over the entity, not its direct location.

Mr. GREEN. So the obstacle is just the cost and the time frame. But is there a way that those four agencies have identified that they can make sure what they are purchasing has not been either compromised—or to the point of maybe even the quality, not to the point—I am not saying sabotaged but the quality would not be to the level we expect.

Mr. WILSHUSEN. Well, one of the activities that these four agencies are conducting to an extent are threat assessments on certain level of acquisitions. Typically, these may be for the most highly sensitive acquisitions, and these threat assessments are for a particular product or service on a particular acquisition. And those threat assessments are then considered and, in some instances, are being provided to a database or repository that is being kept by the Office of the National Counterintelligence Executive.

Mr. GREEN. OK, Mr. Komaroff and Mr. Vega, what are your agencies doing to address some of these obstacles on the quality or the concern of the products we are using?

Mr. KOMAROFF. Do you want to go first?

Mr. VEGA. Sir, so at the Department of Energy, we rely on most of our competitively purchased IT commodity items. We rely on the General Services Administration through their contracting process

to deliver those to the Department of Energy. While there is some assurance, I believe, in the processes at GSA to validate pedigree of some of these devices and technologies, we understand that there is more we can be doing.

I will tell you that we are very much engaged with the Office of the National Counterintelligence Executive in some piloted procurement working groups to help—to better help understand what the actual threat to the Department of Energy is when dealing with some of these manufacturers.

Mr. GREEN. Mr. Chairman, given our Nation's reliance on components manufactured outside the U.S., I think it is important that we do everything in our power to ensure that, at the very minimum, we know where the threats may lie. It is important for manufactures to be up front about where the products they sell come from. It is also important for Federal agencies to carefully vet the products they purchase. Securing our supply chain is not simply a private-sector problem or Federal Government agency problem, because it really affects all of us. And so I appreciate the chance to have this hearing.

Mr. STEARNS. I thank the gentleman.

And the gentleman from Georgia is recognized for 5 minutes.

Mr. GINGREY. Mr. Chairman, thank you.

Mr. Vega, last year, Bruce Held, the DOE's Director of Intelligence and Counterintelligence, noted that if a malicious actor controls your hardware or software, they control your system. Held went on to explain that the military does check the hardware and software in these systems to security vulnerabilities and possibly malicious code but that this would be very costly for the private-sector companies. Do you agree with Mr. Held?

Mr. VEGA. I do agree with Mr. Held.

Mr. GINGREY. Are the IT products and service providers that you deal with checking their products?

Mr. VEGA. Sir, I would have to answer that I believe some of our vendors have programs to vet their supply chains, and some do not.

Mr. GINGREY. And are you attempting to verify that they do? Is that part of what you are doing?

Mr. VEGA. I think what we are doing, sir, is we are embarking on the process of developing explicit direction to our IT purchasers across the Department to do exactly that.

Mr. GINGREY. Has DOE ever identified a cyber incident or control systems incident that could be attributed to corrupted hardware or software linked to a supply chain vulnerability?

Mr. VEGA. Sir, I would have to say in my short time at DOE I have not been made aware of any confirmed supply chain threat that has been realized at the Department. Doesn't mean there isn't. I am just not aware of one.

Mr. GINGREY. And you told us in your opening testimony you have been with DOE in this position for how long?

Mr. VEGA. A little bit more than 8 months, sir.

Mr. GINGREY. And before that?

Mr. VEGA. I was the Chief Information Security Officer at Immigration and Customs Enforcement in the Department of Homeland Security.

Mr. GINGREY. Thank you, Mr. Vega.

Mr. VEGA. Thank you.

Mr. GINGREY. I want to direct the next question, Mr. Chairman, to Mr. Wilshusen.

To what extent will your report, the GAO's report work, shed light on critical infrastructure security? What role does the Department of Homeland Security, for example, have in coordinating information over supply chain challenges?

Mr. WILSHUSEN. Well, with regard to your first question, with regard to the critical infrastructure protection in that, it would address it to the extent that as it relates to IT supply chain, the threats and vulnerabilities. What we found with regard to the supply chains that affect Federal systems and Federal agencieswould also likely affect private sector, because it is generally coming from the same global supply chain area.

Mr. WILSHUSEN. And so in that respect it would be similar.

Mr. GINGREY. Well, you know, it is one thing to ensure standards for off-the-shelf software used by U.S. Government, but how do you communicate supply chain risk to the purchases of specialized control systems software made internationally for use in very critical infrastructure?

Mr. WILSHUSEN. Well, in terms of standards, the Federal Government is pretty much just setting up for what its agencies need to do in terms of securing its software, but if a particular agency needs a particular security requirement on its products and it is acquiring those from a private sector organization, it would typically identify what those are in the contractual mechanisms that exist with that particular company to determine we need these particular security requirements in our software, in our hardware, in our systems, and then assure that the private sector organization is able to deliver.

Mr. GINGREY. What metrics do you have in measuring progress on this front?

Mr. WILSHUSEN. I am not sure there are that many metrics in that particular area that exist.

In terms of percentage of contracts that have security requirements, I don't know of that.

Mr. GINGREY. Mr. Chairman, that's all the questions that I have, and I yield back the last minute.

Mr. STEARNS. I thank the gentleman. I think Mr. Gingrey made a good point, Mr. Vega. Will the Department of Energy finish its process of giving guidance to your suppliers for them to promote their supply chain's integrity? When is that date going to be?

Mr. VEGA. Sir, it is hard to predict how long it will take for the Department.

Mr. STEARNS. Isn't DOE in charge of our nuclear stockpiles?

Mr. VEGA. Yes, they are, sir.

Mr. STEARNS. OK. It seems like you should have an answer. I mean that's a strategic area that we want to be sure that you are protecting, and yet I would just like to actually get a date of when you are going to do something.

Mr. VEGA. Absolutely, our current——

Mr. STEARNS. This whole process.

Mr. VEGA. I am sorry. Our current risk management policy requires our under secretary organizations to account for supply chain risks within their risk management.

Mr. STEARNS. So you don't have a date then? Huh? That's OK, I understand. How long has this been going on then.

Mr. VEGA. I'm sorry, how long has what been going on, sir?

Mr. STEARNS. This whole process of trying to figure out, to give guidance to your suppliers. You can't give a date when you are going to complete it. Have you started it?

Mr. VEGA. We have started engaging the various programs——

Mr. STEARNS. Engaging? You started engaging.

Mr. VEGA. We have started engaging.

Mr. STEARNS. And how long has this process been going on?

Mr. VEGA. It has been going on since we were first contacted by GAO.

Mr. STEARNS. Which is when, how long ago?

Mr. VEGA. Since March of this year.

Mr. STEARNS. OK. So you have only started this month—this month you just started the whole process of guiding guidance to your suppliers to promote the supply chain integrity. So you have only being doing it for 2 weeks, is that true?

Mr. VEGA. With regard to the findings for the GAO report, that is true. However, there are a lot of other activities ongoing within the Department.

Mr. STEARNS. Because I think many of us are concerned that the GAO report shows that DOE is the furthest behind in developing IT supply. You have confirmed it today that it is only the last couple weeks that you've even thought about giving guidance to your suppliers dealing with supply chain integrity.

Let me ask this question.

Ms. DEGETTE. Can I just follow up?

Mr. STEARNS. Well, you can take your own time. You can have a second time on this.

Ms. DEGETTE. But I just want to——

Mr. STEARNS. The gentlelady will suspend. I am involved with a question here.

For example, DOD is in the process of using its intelligence authority in its procurement process. Does the Department of Energy have enough information, enough information to evaluate its vendors or could you benefit from more information?

Mr. VEGA. We can always benefit from more information, and we could always benefit from better collaboration. I will tell you that we are engaged in the interagency very actively with DOD, DHS, and the White House to share information and best practices, not only internally with DOE but also with our Office of Electricity Delivery and Energy Reliability.

Mr. STEARNS. OK. I think what happened is Mr. Gingrey had time and they kept my time, so I still have more time in the original 5 minutes which I was taking. So I assume I have another 2 minutes or so.

Let me ask you this, Mr. Vega. Are you aware of any cyber attacks or threats to DOE systems that were because of a vulnerability a supply chain?

Mr. VEGA. I am unaware of any.

Mr. STEARNS. OK. What types of supply chain threats has the DOE ever faced?

Mr. VEGA. Well, I think we faced supply chain risk to our nuclear surety program.

Mr. STEARNS. To your what program?

Mr. VEGA. To our nuclear surety program.

Mr. STEARNS. How about your nuclear stockpile program, have you—yes or no.

Mr. VEGA. Yes, which is why the Department actually operates two trusted foundries at both Kansas City and Sandia to provide for the surety of that mission.

Mr. STEARNS. Well, based upon this I think you should have been ahead of curve instead of just the last 2 weeks giving guide against to the suppliers.

What specifically is DOE doing to partner with industrial control system manufacturers and energy critical infrastructure operators to identify and mitigate risk to industrial control systems?

Mr. VEGA. Our organization has been working closely with the Office of Electricity Delivery and Energy Reliability to share lessons learned and best practices at the Department with the sector on control systems. However, that organization is led by an assistant secretary, Assistant Secretary Hoffman. I would be glad to take your questions back for the record to get more information on the lessons learned.

Mr. STEARNS. All right. What is the one risk or threat to Federal IT supply chains you are most concerned about and what are you doing to address it?

Mr. VEGA. I'm sorry, I couldn't hear the beginning of your question.

Mr. STEARNS. What is the one risk or threat to Federal IT supply chains you are most concerned about at DOE?

Mr. VEGA. I can't say that I am concerned more about a specific IT supply chain risk. I think we have heard many from our panelists here. There are many that can be manifested in our environment if we are not careful. As I said in my remarks, we have spent a lot of time and energy developing foundational elements to help us detect, mitigate and respond to that threat as well as many other threats we are facing.

Mr. STEARNS. I think we will recognize Ms. DeGette.

Ms. DEGETTE. Mr. Chairman, I was just trying to follow up on the question you were asking of Mr. Vega. Mr. Vega, you said that you guys have just started this process with the contractors this month, correct?

Mr. VEGA. In response to the GAO report, that is correct.

Ms. DEGETTE. And so when do you expect that process to be completed?

Mr. VEGA. We have—we expect that process to follow our internal——

Ms. DEGETTE. Yes, I understand that, but when do you expect it to be completed? You wouldn't give the chairman a date, but perhaps you have a time frame.

Mr. VEGA. I would say, Ms. DeJette——

Ms. DEGETTE. It's DeGette.

Mr. VEGA. I'm sorry, I apologize.

Ms. DEGETTE. That's OK.

Mr. VEGA. Beginning of next calendar year we would have some good progress made.

Ms. DEGETTE. Well, OK. What does that mean, "good progress made"?

Mr. VEGA. The Department of Energy is a very diverse organization with varying missions and varying threats of varying appetites for threat and risk. The idea that the Department can quickly issue policies, procedures, and monitoring systems for that entire complex in a short amount of time is probably not a good assumption.

Ms. DEGETTE. But Mr. Vega, here's our concern, and I think I can say the chairman shares this concern, is we understand all the complexities of the DOE, and this is what I was talking to Mr. Wilshusen about earlier, is that if there are threats we need to identify them, we need to identify the severity and where they occur so that we can begin addressing them. And vague answers like this are very disconcerting to people on both sides of this panel because, after all, it is the Department of Defense.

So I think my suggestion—I am sorry, the Department of Energy. And so what I would suggest is that you folks, now you have got this GAO recommendation and you are putting a process into place, I would suggest that you put a clear timeline into place about goals and results culminating at the earliest possible convenience. We don't want corners to be cut or anything like that. But we think—and then work with this committee to inform us about what the plan is. I think our concern is that the plan seems a little vague just sitting here today.

And with that, I will yield back.

[The information follows:]

COMMITTEE: HOUSE ENERGY AND COMMERCE
SUBCOMMITTEE: OVERSIGHT AND INVESTIGATIONS

HEARING DATE: MARCH 27, 2012

WITNESS: GIL VEGA
PAGE: 14, LINE: 6

INSERT FOR THE RECORD

The Department of Energy (DOE) and its National laboratories and plants are actively working to detect and manage sophisticated supply chain exploits. Across the Department, the supply chain controls specified in Committee on National Security Systems (CNSS) 1253 are implemented and monitored for all classified systems, as required. National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 supply chain controls are implemented and monitored for all high-impact unclassified systems. The Department is committed to the protection of its information and information systems from all threats and vulnerabilities through strong cybersecurity programs and enhancing its programs where supply chain risk management is concerned.

The Department of Energy (DOE) cybersecurity program is founded on a mission-based Risk Management Approach (RMA) and executed through policies and procedures developed and promulgated through Under Secretary-level Senior Department Management (SDM) organizations. The SDM organizations are responsible for the implementation of DOE policies and are responsible for all relevant requirements and assignments within their subordinate organizational levels through the policy required Risk Management Implementation Plans

(RMIPs). RMIPs establish risk decisions and remediation of security findings accountability at the SDM-level.

To further address the GAO report recommendations, the Office of the Chief Information Officer (OCIO) will develop a DOE Notice, which is an expedited policy directive, to institute IT supply chain risk management programs within SDM organizations. This DOE Notice, to be approved and signed by first quarter fiscal year (FY) 2013, will establish SDM program requirements to include the policies, processes (including contracting and procurement processes), and monitoring capability identified in the GAO recommendations as well as supply chain oversight, mitigation, and remediation appropriate to organizational mission and risk tolerance.

In addition, the OCIO is administering an Agency-wide menu of activities to support organizations in their program development and execution, as well as leveraging these programs to enhance situational awareness across the Department. Examples of such activities include conducting summits (first one is planned for the July/August timeframe of FY 2012), documenting best practices, implementing Agency-wide working groups, and synchronizing with the DOE Joint Cybersecurity Coordination Center. A Department-level supply chain program framework is being developed for the first quarter FY 2013; the implementation plan for the framework will be completed during the second quarter of FY 2013.

Mr. STEARNS. I thank the gentlelady. And Mr. Terry is recognized for 5 minutes.

Mr. TERRY. Thank you, Mr. Chairman. And Mr. Vega, I apologize that I was in—to all three of you—in an anteroom in a quick meeting that lasted a few minutes more. I walked in during your answer and didn't really hear what Mr. Gingrey's question is, so it piqued me, I was really interested.

Just very bluntly then so I am clear in regard to having a cybersecurity plan for a critical infrastructure nuclear power plant, who is best to oversee that cyber plan, DOE or Homeland Security?

Mr. VEGA. Who is best to oversee a cybersecurity plan for a privately owned power generator, is that the question?

Mr. TERRY. OK, let's say a public power nuclear facility. I don't care, it is nuclear.

Mr. VEGA. Right.

Mr. TERRY. And it is under DOE.

Mr. VEGA. It is DOE. I have to say, sir, that my focus on cybersecurity is internal to the Department of Energy and the Federal M&O contractors that operate our National Labs. I am not that familiar to offer an informed opinion about who would be better overseeing the implementation of a cybersecurity plan.

Mr. TERRY. I was hearing that you were saying that perhaps Department of Homeland Security was better prepared to do that, and I am trying to figure out where their nuclear power plant expertise would be.

Mr. VEGA. I am not sure what you heard, sir.

Mr. TERRY. OK. I just want to clarify that.

Evidently—were you suggesting, Mr. Wilshushen? I'm sorry.

Mr. WILSHUSEN. That's OK, Wilshusen.

Mr. TERRY. Wilshusen, just like it is written, I am sorry. Did you suggest that Homeland Security would be better supervising overseeing cybersecurity techniques and plans for nuclear power plants which would obviously, because they are nuclear, would probably be defined as critical?

Mr. WILSHUSEN. I did not suggest that, but I will mention that, and it is not part of this report on IT supply chain, but DHS does have a role in terms of being the sector under the National Infrastructure Protection Plan and program, DHS does have a role in providing guidance and overseeing the—I think it is the nuclear power industry. Also, Nuclear Regulatory Commission would be a member and would have insight into that since they are regulators of these nuclear power plants.

Mr. TERRY. Is the Nuclear Regulatory Commission under Homeland Security's umbrella or another agency's like DOE?

Mr. WILSHUSEN. It is a separate, independent agency of Federal Government.

Mr. TERRY. Independent agency.

Mr. WILSHUSEN. It is separate. And so they also specify some of the security requirements in its role as a regulator of nuclear power plants to give security. They do conduct certain reviews over that.

Mr. TERRY. Well, I am going to ask you one follow-up question that stood out to me during your testimony, but quickly, Homeland Security under my personal view has been a disaster. And to put

them in charge of cybersecurity of any critical infrastructure scares the hell out of me frankly. And every time I go through an airport I think of how incompetent they are. So that's just my statement for the record. I am sorry I was looking at you when I said that.

But you mentioned in the chain, supply chain that we are concerned about the unauthorized, which then led me to the question of how—what needs to be authorized? What parts of the supply chain, is it the individual parts at the assembly? Who is going to be able to have the authority to say that they are authorized to approved that this chip can go into this computer, that can be sold then to the Defense Department. I can't get my mind around who would have that level of authority, and you have 28 seconds.

Mr. WILSHUSEN. First of all, when I mentioned the word "unauthorized" it dealt with acquiring products or parts components if you will from unauthorized distributors as opposed to those companies or entities, either the original component manufacturer or their other approved, if you will, suppliers to provide it. So if an agency were to go to some other, through some other distributor that's not authorized to sell a particular product that was the vulnerability to which I was referring.

Mr. TERRY. All right. Thank you.

Mr. STEARNS. All right, we will let the first panel be dismissed and we will have the second panel come up. Thank you very much for your time.

Mr. STEARNS. Welcome the second panel. We have Mr. Larry Castro, Managing Director of the Chertoff Group, and we have Dave Lounsbury, Chief Technical Officer of the Open Group. Welcome each of you. And at your convenience, Mr. Castro, we will let you start with your opening statement.

First we have to swear you in.

As you know, the testimony that you are about to give is subject to Title 18, section 1001 of the United States Code. When holding an investigative hearing this committee has a practice of taking testimony under oath. Do you have any objection to testifying under oath?

Mr. CASTRO. I do not.

Mr. LOUNSBURY. No.

Mr. STEARNS. The chair then advises you that under the rules of the House and the rules of the committee you are entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony today?

Mr. CASTRO. I do not.

Mr. LOUNSBURY. No, sir.

Mr. STEARNS. In that case will you please rise, raise your right hand and I will swear you in.

[Witnesses sworn.]

Mr. STEARNS. Now if you would be so kind as to give your 5-minute opening statement. Mr. Castro, we will start with you. Welcome.

STATEMENTS OF LAWRENCE CASTRO, MANAGING DIRECTOR, THE CHERTOFF GROUP; AND DAVE LOUNSBURY, CHIEF TECHNOLOGY OFFICER, THE OPEN GROUP

STATEMENT OF LARRY CASTRO

Mr. CASTRO. Good morning, Chairman Stearns, Ranking Member DeGette, and members of the subcommittee. I appreciate the opportunity to speak with you today regarding the important role of IT supply chain security and our Nation's approach to cybersecurity. I am appearing today in my personal capacity although for the record I am currently a Managing Director at the Chertoff Group, a firm that provides strategic advisory services on security matters, including cybersecurity.

While my work at Chertoff Group informs much of my current insight into the cybersecurity threat environment, my basic understanding of information assurance in cybersecurity is drawn from my 44 years of Federal service at the National Security Agency. It is thus from these two perspectives that I offer my views for your consideration today.

I commend the subcommittee for addressing this topic today as the GAO report well describes securing the supply chain is a challenging and complex task with many moving parts and dependencies. I would suggest, however, that it is not an intractable problem and it is one that can be addressed in the risk management framework.

The GAO report documents that there's ample policy direction and implementing guidance from which one can start to build supply chain defenses. What is needed, however, is a framework that can build on that policy base and also support the implementation detail. Risk management offers such a framework. Risk management approaches security from the aspects of threats, vulnerabilities and consequences and can be used to unwrap some key supply chain issues.

Let's first consider the threat actors who might both be able to benefit from and execute an infiltration of the supply chain, perhaps by inserting a modified component into the supply chain of a critical U.S. Government IT enterprise. To do so of course the adversary must be capable of penetrating the production process at a point far enough downstream to ensure that the right target has been infiltrated.

In addition to performing the adversary's desired covert function, the modified component must also execute the component's function as originally designed. I would submit to you that across the spectrum of threat actors in cyberspace today the most likely players to have the motive and the capability to successfully accomplish such a deception would be nation-states.

So who then would be the nation-states that might have the necessary qualifications and motives? The GAO report notes as you have heard already in testimony today about an outstanding organization on point within the Federal Government for identifying such threat actors. That organization is the Office of the National Counterintelligence Executive, or NCIX, within the Office of the Director of National Intelligence.

In October 2011 NCIX published this eye opening report to the Congress, entitled Foreign Spies Stealing U.S. Economic Secrets in Cyberspace. The report convincingly presents the case that both the People's Republic of China and the Russian state apparatus have both the intent and capability to undertake economic espionage enhanced by cyber means. These are the key threat actors against whom our supply chain defenses should be aligned.

What consequences do they seek to achieve by infiltrating the U.S. supply chain? The scope of objectives spans the full range of results achievable from malicious activity in cyberspace, some of which you all have already addressed this morning. They include the compromise of confidentiality leading to the loss of sensitive data and intellectual property, the loss of availability of critical national security systems, and the corruption of data residing in these critical systems.

As has already been discussed today, there are numerous vulnerabilities in the supply chain that can be exploited. There are, however, well documented best practices and tools that may be implemented to address some of these vulnerabilities, and I believe the next speaker on the panel will address some of those. The use of these tools and resources, however, must be considered in the context of likely threat actors and the consequences that they seek to achieve.

Finally, I would like to comment about a section of the GAO report again that you already discussed this morning dealing with the lineage of equipment used in U.S. Government networks. While the report concluded that emphasis is not given to determining if such networks contained foreign developed components, the intelligence community representatives quoted in the report offered the view that determining if a relationship exists between the supplier company and a foreign military or intelligence service, that would be a more reliable indicator of a potential security risk than simply ascertaining whether a specific product was manufactured or provisioned outside the United States. I strongly endorse this conclusion and note that the practice of conducting such due diligence audits of supplier sponsor links is well established in the private sector.

For maximum effectiveness, however, this due diligence requires a good conduit to move high fidelity threat actor information between the U.S. Intelligence community and those in the private sector who would benefit from the intelligence community's insights. It is encouraging that many of the cyber bills under consideration by you all this session address the need for such improved information sharing.

Again, thank you for the opportunity to address this topic, and I would be pleased to answer your questions at the appropriate time.

[The prepared statement of Mr. Castro follows:]

Statement of

Mr. Lawrence Castro

Managing Director, The Chertoff Group

to the

House Energy and Commerce Subcommittee on Oversight

March 27, 2012

IT Supply Chain Security: Review of Government and Industry Efforts

Good Morning Chairman Sterns, Representative DeGette and members of the Subcommittee.

I appreciate the opportunity to speak with you today regarding the important role of IT supply chain security in our nation's approach to cybersecurity. I would like to state clearly that I am appearing today in my personal capacity, although, for the record, I am currently a Managing Director at the Chertoff Group, a global security and risk management firm that provides strategic advisory services on a wide range of security matters, including cybersecurity and the supply chain security component of cybersecurity.

While my work at The Chertoff Group certainly informs much of my current insight into the cybersecurity threat environment and the challenges faced by our nation's national security and homeland security sectors, my basic understanding of information assurance and cybersecurity is drawn from my 44 years of Federal service at the National Security Agency. It is from these two perspectives that I offer my views for your consideration today.

I would like to commend the subcommittee for addressing the topic of cybersecurity generally in its hearings and the supply chain security issue specifically today. As the GAO report that was reviewed at the outset of this hearing so well describes, securing the supply chain of products destined to be employed in Federal national security and national security related information systems is a complex task with many moving parts and dependencies. I would suggest, however, that it is not an intractable problem and it is one that can be addressed in a classic risk management framework.

SUMMARY OF PAST WORK

As I noted, the GAO report under discussion today provides both an excellent overview and problem statement. Other efforts have also contributed to the body of literature related to this critical area.

- As the subcommittee's background paper notes the 2008 Comprehensive National Cybersecurity Initiative (CNCI) identified supply chain risk management as one of the effort's 12 critical initiatives.
- The Administration earlier this year published the National Strategy for Global Supply Chain Security[1]. While addressing issues broader than IT, the strategy does provide a range of policy goals that are the basis for further action.
- Two Departmental efforts that were completed in the interim are noteworthy:
    - During Panel One you heard from Mr. Komaroff who leads DoD's Trusted Mission Systems Networks effort that was established by DoD Directive-Type Memorandum 09-016 on March 25, 2010[2].
    - Additionally, in June 2010 NIST completed and documented[3] a comprehensive set of supply chain risk-mitigating best practices that could be applied on a pilot basis to 'jumpstart' specific Department or Agency efforts.
- The private sector has been active in this area as well. In addition to the Open Group's work which is being discussed today, the Internet Security Alliance has published draft guidelines for securing the supply chain for electronic components[4].

Thus, there is ample policy direction and implementing guidance from which one can start to build supply chain defenses. What is needed, however, is a framework that can build on the policy base and also can support the implementation detail. Risk management offers such a framework.

APPROACHING SUPPLY CHAIN SECURITY THROUGH A RISK MANAGEMENT CONSTRUCT

Risk management approaches security from the aspects of threats, vulnerabilities and consequences, and can be used to unwrap some key supply chain issues.

---

[1] The White House, *National Strategy for Global Supply Chain Security*, January 23, 2012
[2] DTM 09-016, Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems, March 25, 2012
[3] NIST draft NISTIR 7622, *Piloting Supply Chain Risk Management Practices for Federal Information Systems*, June 2010
[4] Internet Security Alliance (ISA), *The ISA Guidelines for Securing the Electronics Supply Chain*, Draft Version 6, 2011.

Threat Actors

Let's first consider who might both be able to benefit from and execute an infiltration of the supply chain, perhaps by successfully inserting a modified component into the supply chain of a critical U.S. government IT enterprise. To do so, an adversary must be capable of penetrating the production process at a point far enough downstream in the process to ensure the right target has been infiltrated. In addition to performing the adversary's desired covert function, the modified component must also precisely execute the component's function as originally designed. I submit that across the spectrum of threat actors active in cyberspace, the most likely players to have the motive and the capability to successfully accomplish such a deception would be nation states. The simple substitution of counterfeit components capable of performing the original design intent but which present the risk of lower reliability or performance must not be overlooked, but I believe it is of secondary consideration.

Who then would be the nation states that have the necessary qualifications and motives? The GAO report notes the existence of an outstanding organization which is on point within the Federal Government for identifying such threat actors. This organization is the Office of the National Counterintelligence Executive (NCIX) within the Office of the Director of National Intelligence. In October 2011, NCIX published an eye-opening report to Congress entitled "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace".[5] The report convincingly presents the case that both the People's Republic of China and the Russian state apparatus have both the intent and capability to undertake economic espionage enhanced by cyber means. The Chinese and the Russians, therefore, are the key threat actors against whom our supply chain defenses must be aligned.

Consequences

What then do these nation state adversaries seek to achieve by compromising the U.S. supply chain? The scope of objectives spans the full range of those who engage in malicious activity in cyberspace:

- **Compromise of Confidentiality** leading to the loss of sensitive data and intellectual property (IP).
- **Loss of Availability** resulting from sabotage of Internet-enabled technologies and critical communications systems.
- **Degradation of Data Integrity** that would result in lack of confidence in sensor or weapons systems-related data in the lead up to or during conflict.

[5] Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011.* October 2011.

The NCIX report gives prominence to the extensive loss of IP resulting from Chinese and Russian cyber espionage activity, and this most certainly is the near-term consequence of concern. The loss of availability and data integrity, however, are longer-term impacts which must be acknowledged in building the defensive strategy.

Vulnerabilities

There are numerous vulnerabilities in supply chains for both hardware components and supporting software that the sophisticated nation state adversary can pursue. As noted earlier, there are both NIST and industry best practices and tools that may be implemented to address these vulnerabilities. Additionally, the DHS National Cybersecurity Division's (NCSD) Supply Chain Risk Management Program (also described in the GAO report) offers government users an array of useful services to apply. The use of these tools and resources, however, must be considered in the context of the likely threat actors and the consequences they seek to achieve in executing what is certainly an extensive, resource intensive, intelligence-driven covert action by our potential adversaries.

HOW IT ARCHITECTURE CAN ADDRESS THE THREAT

For IT enterprises either in operation or under design, considerations of system architecture can contribute to supply chain risk mitigation. Two such considerations are worthy of discussion.

Presumption of Breach

This concept, first announced last summer in the DoD Strategy for Operating in Cyberspace[6], posits that one should begin considerations of cybersecurity with the assumption that one's network is already breached and as such, must employ defenses capable of "operating under attack". Such a notion is a powerful one that requires the cyber defender to consider defense mechanisms beyond the standard firewall/anti-virus regime and good computer user hygiene.

Data Centric Defense

If one begins with the premise that a supply chain vulnerability has been exploited and as a consequence the adversary is now present in the IT enterprise, one is quickly driven to the following approach to protect against the loss of critical information:

[6] *Department of Defense Strategy for Operating in Cyberspace*. July 2011. http://www.defense.gov/news/d20110714cyber.pdf

- First, it is necessary to catalog and consolidate the information that is determined to be the most critical to the operation of the element the IT enterprise supports. These are the so-called "crown jewels".
- Next, one establishes virtual enclaves within which this mission critical data is stored and is afforded special protection (e.g. by encrypting data at rest).
- Access to this critical data is then restricted by robust authentication mechanisms to only those with a "need to know". The activity of these users is strictly monitored, particularly with regard to movement of this critical data outside of the protected enclave.

Thus, even though the adversary may have established a presence within our network and gained the privileges of a legitimate user, attempts to steal and exfiltrate data will be detected.

INTELLIGENCE AND INFORMATION SHARING AS AN ENABLER

Finally, I would like to comment about a section of the GAO report dealing with "lineage" of equipment and software used in U.S. government networks. The report concluded that emphasis is not given to determining if such networks contain foreign-developed equipment or software, or are supported by foreign-based services. The report noted that both ODNI and NSA representatives offered the view that determining if a relationship exists between a supplier company and a foreign military or intelligence service is a more reliable indicator of a potential security risk than whether a product was manufactured or provisioned outside the United States. I would strongly endorse this conclusion and would note that the practice of conducting "due diligence" audits of such links is well established in private sector best practices and is currently based primarily on open source information.

The challenge, of course, is that for maximum effectiveness, this "due diligence" requires a good conduit of threat actor information between the U.S. Intelligence Community, which has the highest fidelity information in this regard, and those in the private sector who would benefit from the Intelligence Community's insights. It is encouraging that many of the cybersecurity bills under consideration by the Congress address the need for such improved information sharing.

Again, thank you for the opportunity to address this critical topic and I would be pleased to address your questions.

###

Mr. STEARNS. I thank you. Mr. Lounsbury, your opening statement, please.

STATEMENT OF DAVE LOUNSBURY

Mr. LOUNSBURY. Chairman Stearns, Ranking Member DeGette, and distinguished members of the committee. On behalf of the Open Group and the Open Group Trusted Technology Forum, I want to thank you for the opportunity to speak at this IT supply chain security hearing to discuss how the Open Group's Trusted Technology Forum plans to address some of the challenges in securing the global supply chain that have been discussed today.

A little background: The Open Group is a global consortium that enables the achievement of business objectives through IT standards. We have more than 400 members, spanning all sectors of the IT community from customers to vendors, to integrators and consultants as well as academics and researchers. And staff works with them to capture, understand, and address their current and emerging requirements and establish the policies, shared best practices, to facilitate interoperability and develop consensus around evolving and integrating standards. And to back this we operate an industry premier certification service operating a variety of certification programs over 20 years.

In 2008, the then current Under Secretary for the Department of Defense Acquisition Technology and Logistics posed the follow challenge to the Open Group members: How can the DOD safely procure IT technology from an increasingly global and sometimes unpredictable supply chain in a rapidly changing threat environment? The discussion focused on the challenges associated with an increased reliance on commercial-off-the-shelf information communication technologies in commercial and government enterprise, including the defense industry. The parties formalized those discussions in an initiative under the Open Group that we call the Open Trusted Technology Forum. And that is a forum, it is a global initiative that brings in government industry and other interested participants to work to develop an open technology, open trusted technology provider standard that's a public-private partnership to address this very clear cybersecurity challenge in a shared, multistakeholder risk environment like the global supply chain.

Member organizations contributing to the work include a broad range of global suppliers, buyers of products and third party test labs. The open trusted technology provider standard, which is currently published as a snapshot, provides organization commercial best practices that when properly adhered to will enhance the security of the global supply chain and the integrity of COTS ICT products throughout the entirety of the product lifecycle. That is from the design phase through the sourcing of the components, build, fulfillment, distribution, sustainment and all the way to the disposal phase.

Snapshot was released in March and is intended to become an Open Group standard which will be available to everyone, and this provides a set of best practice requirements and recommendation on two types of risk inherent in the acquisition and use of COTS ICT products. First is tainted product risk, and that is a product

is produced by the provider and is acquired through legitimate reputable channels but has been tampered with maliciously.

The second is the counterfeit product risk where a product is produced other than by or for the provider or is supplied by other than a reputable channel and is presented as being legitimate.

The standards based on best practices have been contributed from the experience of very mature industry providers and the results rigorously reviewed through an open consensus process, standards sufficiently detailed and prescriptive enough to be useful in raising the bar for all the technology suppliers, and it really lends itself to an accreditation process that will provide assurance that it's being followed in a meaningful and repeatable manner. And by adopting the standard and committing to conform to these best practices, technology providers, whether it be hardware or software component suppliers and integrators, will help ensure the integrity of the COTS ICT products.

Now given the very fast pace changes of technology and risk landscape, the OTPF plans to evolve the OTPF standard over time, and so as specific threats emerge or the market needs evolve then the forum will update the standard to address these threats or changes.

It takes a very comprehensive view about the practices a provider should follow in order to be considered to be a trusted technology provider that builds with integrity allowing its customers to buy with confidence.

Chairman Stearns, Ranking Member DeGette, and members of the committee, thank you again for the opportunity. I want to offer up the expertise of the Open Trusted Technology Forum to the subcommittee and other congressional committees as they continue to examine supply chain issues. We look forward to working together to address the critical problem of improving global supply chain security.

Thank you.

[The prepared statement of Mr. Lounsbury follows:]

Executive Summary of
The Open Group's testimony to the House Energy and Commerce
Oversight and Investigations Subcommittee Hearing on
IT Supply Chain Security: Review of Government and Industry Efforts

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. We will present the work undertaken by The Open Group Trusted Technology Forum (OTTF) to address a clear cybersecurity challenge in the shared, multi-stakeholder risk environment of the global supply chain.

The OTTF is developing the Open-Trusted Technology Provider Standard to provide organizational commercial best practices that, when properly adhered to, will enhance the security of the global supply chain and the integrity of COTS ICT products throughout the entirety of the product life cycle; through design, sourcing, build, fulfillment, distribution, sustainment, and disposal phases. By adopting the Standard, and by committing to conform to these best practices, technology providers, hardware and software component suppliers and integrators of all sizes, will help assure the integrity of their COTS ICT products. Organizations that demonstrate their conformance through a planned accreditation program will be considered a certified Trusted Technology Provider that "builds with integrity", allowing customers to "buy with confidence".

STATEMENT of

David Lounsbury, Chief Technology Officer, The Open Group on behalf of The Open Group and The Open Group Trusted Technology Forum

Submitted for the record

House Energy and Commerce Oversight and Investigations Subcommittee

Hearing on

IT Supply Chain Security: Review of Government and Industry Efforts

March 27, 2012

Chairman Upton, Ranking Member Waxman and distinguished members of the Committee:

On behalf of The Open Group and the Open Group Trusted Technology Forum, I am pleased to submit the following statement for the record of the hearing entitled: IT Supply Chain Security: Review of Government and Industry Efforts, held on March 27, 2012. The Open Group was invited to discuss The Open Group Trusted Technology Forum's plans to address some of the challenges in securing the global supply chain.

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 400 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community;

©2012 The Open Group

customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers. The Open Group staff works with our members and other constituencies in order to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

The Open Group Trusted Technology Forum (OTTF)

The Open Group Trusted Technology Forum, a forum of The Open Group, is a global initiative that invites industry, government, and other interested participants to work together to evolve the Open-Trusted Technology Provider Standard (the Standard), currently published as a "snapshot", which is a draft version of what is intended to become a final open standard. The snapshot provides organizational commercial best practices that, when properly adhered to, will enhance the security of the global supply chain and the integrity of Commercial Off –the- Shelf (COTS) Information and Communication Technology (ICT) products. It provides a set of guidelines and best practice requirements and recommendations that help assure against tainted and counterfeit products (discussed below) throughout the entirety

of the COTS ICT product life cycle; through design, sourcing, build, fulfillment, distribution, sustainment, and disposal phases.

The snapshot was released on March 9, 2012 and is intended to become an Open Trusted Technology Provider Standard, after evaluating initial feedback on the snapshot, developing conformance criteria to demonstrate adherence, and defining an accreditation program. The snapshot and the subsequent published versions of the Standard are open standards and can be downloaded free of charge from The Open Group's website to help assure broad adoption globally.

Given the fast-moving pace of change in technology and the risk landscape, The Open Group Trusted Technology Forum (OTTF or "The Forum") plans to take a dynamic and phased approach, staging additional standards over time. As threats change or market needs evolve, the Forum intends to update the Standard by releasing addenda to address new specific threats or market needs.

The Open Trusted Technology Forum is a government-industry partnership.

The Forum is an effective example of a cooperative, public/private partnership working effectively to address a clear cybersecurity challenge in a shared, multi-stakeholder risk environment, such as the global supply chain. The Forum was initiated through informal discussions organized by The Open Group between government and industry where the then current Undersecretary for Department of Defense (DoD)/Acquisition Technology & Logistics (AT&L) posed the following question: "How can the DoD safely procure IT technology from an increasingly global supply chain?" The discussions focused on the challenges associated with an

©2012 The Open Group

increased reliance on the use of COTS ICT products in commercial enterprises and governments, including the defense industry, challenges compounded by the fact that these products rely on a sometimes unpredictable supply chain in a rapidly-changing threat environment.

The parties involved in the early discussions then formalized an initiative under The Open Group as the Open Group Trusted Technology Forum. The Forum member organizations currently are: Apex Assurance, atsec Information Security, Boeing, Booz Allen Hamilton, CA Technologies, Carnegie Mellon University Software Engineering Institute (SEI), Cisco, EMC, Fraunhofer SIT, Hewlett-Packard, IBM, IDA, Juniper Networks, Shenzhen Kingdee Middleware, Lockheed Martin, MITRE, Microsoft, Motorola Solutions, NASA, Oracle, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD AT&L), SAIC, Tata Consultancy Services, and the U.S. Department of Defense/CIO.

The Forum participants recognize the value the Standard can bring to governments and commercial customers worldwide, particularly since the Standard itself is informed by the practical experience and knowledge of a wide range of individuals from customer, vendor and other organizations. Customer organizations can incorporate consideration of this standard into their sourcing and procurement strategies, as appropriate.

The recent release of the snapshot of the Standard allows:

- acquirers and customers to begin consideration of how this standard fits into their procurement and sourcing strategies, and to consider recommending

the adoption of the best practice requirements to their providers and integrators.

- providers, component suppliers, and integrators to begin planning for the eventual implementation of the Standard in their organizations

The Standard is aimed at enhancing the security of the global supply chain

Adopting best practices that have been taken from the experience of mature industry providers, rigorously reviewed through a consensus process, and established as requirements and recommendations in the Standard will provide significant advantage in helping reduce risk. By adopting this Standard, and by committing to conform to these best practices, technology providers, large and small, hardware and software component suppliers and integrators, will help assure the integrity of their COTS ICT products. This Standard is sufficiently detailed and prescriptive to be useful in raising the bar for all providers and lends itself to an accreditation process to provide assurance that it is being followed in a meaningful and repeatable manner.

The initial version of the Standard addresses two types of risks inherent in the acquisition and use of COTS ICT products:

- Tainted product risk – a product is produced by the provider and is acquired through reputable channels, but has been tampered with maliciously.

- Counterfeit product risk – a product is produced other than by, or for, the provider, or is supplied by other than a reputable channel, and is presented as being legitimate.

The Forum takes a comprehensive view about the best practices a provider should follow. The Standard specifies practices that providers can incorporate in their own internal product life cycle processes, i.e. that portion of product development that is "in-house" and over which they have relatively direct operational control. Additionally, the Standard describes supply chain security practices that should be followed when a provider is incorporating third-party hardware or software components, or when depending on external manufacturing and delivery or supportive services.

The value of this approach is that it is process-focused, and thus will be horizontally integrated into a company's business processes. While there may be existing standards in the industry that have requirements for designing and implementing security driven functionality and where there is corresponding evaluation on a per product version basis, this Standard is intended to provide a broader perspective, with assurances that products have not been tainted or corrupted with counterfeit components while being developed or manufactured in the global supply chain. So although a product version may pass an evaluation – what happens in the development and production of that product is a different scenario and one that the Forum is addressing in the Standard.

Conformance Criteria and Accreditation

The Forum is in the process of defining conformance criteria and an accreditation program that will allow providers who meet the Standard's conformance criteria to become accredited and acknowledged on a public accreditation registry. Customers from industry and government can then use the registry to identify Trusted Technology Providers with increased confidence.

Adoption of these best practices and conformance criteria by component suppliers, by providers who include those components in their products, and by integrators who integrate components and products, will enable industry and government to manage commercial supply chain risk sustainably in a dynamic and globally-integrated environment. Thus, enabling Trusted Technology Providers to "build with integrity", and customers to "buy with confidence".

The Open Group has been acting as a vendor-neutral certification authority business for over 20 years - working with their forums to develop and operate certification programs, and working with other 3rd party consortia to develop and operate their certification programs as a vendor-neutral third party. The Open Group offers certification programs for: product certifications, skills and capabilities certifications, and best practice certifications. Some examples include: Unix®, TOGAF®, OpenCA (Certified Architect), OpenCITS (Certified IT Specialist), North American State and Provincial Lottery Association (NASPL), and one of our most recent for the NFC Forum. In some of these programs, the Open Group acts as the validator and for others we utilize third party laboratories for validations. For all of

them The Open Group operates and administers the certification program as the vendor-neutral 3rd party.

Standards Harmonization and Global Outreach is required

The Open Group leverages existing open standards to the greatest extent possible, including international standards such as International Organization for Standardization (ISO) and has recognized PAS (Publicly Available Specification) submitter status to ISO, which allows The Open Group to send specifications directly for country voting, to become ISO/IEC standards.

One important element of the Forum's work is our commitment to complement and interoperate with other relevant standards and industry practices. International standardization of the Standard is an important objective of their effort. Thus, last year the Forum's Standards Harmonization Work Stream conducted a review of the supply chain standards landscape. The Work Stream found that there were no other standards that covered the breadth of the Standard and no standard that addressed the depth of the Standard supply chain best practices. The Work Stream members did, however, identify standards and standards-type activities that had small areas of overlap. Given the desire to help assure that the standards would be harmonized and aligned as much as possible, the Forum is establishing liaisons and relationships with a range of organizations and working groups including:

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1,

Information Technology Standards, Subcommittee 27, IT Security Techniques – where we have pending liaisons in two SC27 Working Groups:

  - WG3, Security Evaluation Criteria, which produces Common Criteria-related standards such as ISO/IEC 15408 and ISO/IEC 18045:
  - Working Group 4 (WG4), Security Controls and Services, which is producing ISO/IEC 27036 on Information Security for Supplier Relations

- InterNational Committee for Information Technology Standards (INCITS-CS1)
- National Security Agency (NSA)
- National Information Assurance Partnership (NIAP)
- National Institute of Standards and Technology (NIST)
- Communications-Electronics Security Group (CESG) - UK

The Forum is working globally with governments and international standards organizations to promote and harmonize this and future Standards directed at supply chain. The Forum wishes, where appropriate, to leverage existing evaluation and testing schemes while harmonizing with the security standards to which those schemes relate.

Conclusion:

Thank you for the opportunity to provide an overview of how The Open Group Trusted Technology Forum is addressing supply chain security. We offer up the expertise of the Forum to the Subcommittee and other Congressional committees as

they continue to examine supply chain issues. For additional information please feel free to contact me at d.lounsbury@opengroup.org. For a further look at The Open Group and to download the Snapshot please access the following links: The Open Group and The Open Trusted Technology Provider Standard Snapshot.

The Open Group® is a registered trademark of The Open Group.

Appendix: Security Activities of The Open Group

Assuring the security of corporate data, information systems and critical infrastructure is a challenging task, requiring the joint efforts of customers, software and platform vendors, and governments. The Open Group hosts a variety of Forums, Work Groups and projects that address various aspects of the challenge of security.

The Security Forum focuses on Security Architecture and Information Security Management. The forum produces technical standards, guides, best practices, and other deliverables aimed at customer practitioners and vendors.

The Jericho Forum® provides thought leadership on enabling businesses to securely collaborate in a deperimeterized world. The Jericho Forum produces position papers, requirements, and guidance for customer organizations and security vendors.

The Real-time & Embedded Systems Forum provides core technology suppliers, integrators and customers with dependability through assuredness in the development of secure, reliable systems using open standards. The Forum delivers whitepapers, technical API standards, guides, and evaluation and certification programs.

The Open Group Trusted Technology Forum (OTTF) leads the development of a standard, which is a set of best practices for product engineering, secure development and supply-chain security. This standard is called the Open Trusted Technology Provider Standard (O-TTPS). The Forum is also working on marked accreditation and conformance programs for provider organizations that conform to the O-TTPS standard.

The Cloud Computing Work Group is doing work in the area of security for the Cloud and SOA. This group is working on reference architecture for Cloud security.

The Open Group's security-related projects and events:

- **Information Security Management:** The Open Group Information Security Management Maturity Model (O-ISM3) project strives to continually improve information security management. Our goal is to further develop O-ISM3, and to establish it as an open industry standard
- **Risk Management:** Risk management is fundamental to effectively securing information, IT assets, and critical business processes. The Open Group has produced important publications and projects in this business-critical area
- **Security Architecture:** As a hub where expertise in architecture development and security converge, The Open Group is uniquely qualified to lead the industry in establishing consistent, reliable standards for developing secure architectures
- **Security Standards:** With a long legacy in the development of important security standards, The Open Group continues to create security standards that promote the development of secure IT systems
- **Security Conferences:** The Open Group produces and hosts quarterly security conferences, held jointly with our Enterprise Architecture Practitioners

©2012 The Open Group

conferences. These events provide an interactive forum that fosters in-depth discussions with security leaders, and meaningful networking with peers.

Examples of published works include:

Security Certification Product Standards

X98SS Secure Communications Services

X98XS Baseline Security 98

Consortium Specifications

H072 Enterprise-Wide Security: Authentication & Single Sign-On

H073 Business Services Architecture

H074 Interoperability: Electronic Mail Systems

H075 Interoperability

H076 Enterprise-Wide Security

H077 Enterprise Directory Services Integration

Corrigenda

U039 X/Open Single Sign-On Service (XSSO) - Pluggable Authentication

U051 CDSA/CSSM Authentication: Human Recognition Service (HRS) API

Guides

G033 Manager's Guide to Data Privacy

G044 Introduction to Security Design Patterns

G052 Guide to Digital Rights Management

G061 Framework for Control over Electronic Chattel Paper

G081 Requirements for Risk Assessment Methodologies

G112 Open Enterprise Security Architecture (O-ESA)

G250 Manager's Guide to Information Security

G905 CDSA Explained, Second Edition

Preliminary Specifications

P441 Distributed Audit Service (XDAS)

P442 Generic Cryptographic Service API (GCS-API) Base

P702 X/Open Single Sign-On Service (XSSO) - Pluggable Authentication

Snapshots

S020 Security Interface Specifications: Auditing and Authentication

S307 GSS-API Security Attribute and Delegation Extensions

Technical Guides

C103 FAIR - ISO/IEC 27005 Cookbook

G031 Security Design Patterns

G206 Defining and Buying Secure Open Systems

G410 Distributed Security Framework (XDSF)

G801 Architecture for Public-Key Infrastructure (APKI)

Security Technical Standards

C013 CDSA/CSSM Authentication: Human Recognition Service (HRS) API V2

C081 Risk Taxonomy

C102 Open Information Security Management Maturity Model (O-ISM3)

C111 Open Automated Compliance Expert Markup Language (O-ACEML)

C441 Generic Security Service API (GSS-API) Base

C529 X/Open Baseline Security Services (XBSS)

C908 Authorization (AZN) API

C914 Common Security: CDSA and CSSM, Version 2 (with corrigenda)

C425 Systems Management: Backup Services API (XBSA)

Security Technical Studies

E605 Security in Federated Naming

E403 Security in Interworking Specifications

E503 Desktop Security

©2012 The Open Group

White Papers

W031 Intrusion Attack and Response Workshop (inc. Full Script)

W031A Intrusion Attack and Response Workshop

W075 Information Security Strategy, Version 1.0

W117 TOGAF® and SABSA Integration

W119 Security Principles for Cloud and SOA

W055 Guide to Security Architecture in TOGAF®ADM

W116 An Architectural View of Security for Cloud

Mr. STEARNS. And I thank you. And I will start with my first set of questions. I will ask you the first question that I am trying to get an answer to, which I asked the first panel, to each of you. Is the biggest emerging cybersecurity threat to consumers and government agency the cybersecurity threats to the supply chain, IT supply chain? Yes or no. Do you want me to repeat the question? Is the biggest emerging cybersecurity threat to consumers and government agencies the cybersecurity threats to the IT supply chain? Yes or no.

Mr. CASTRO. My answer would be no.

Mr. STEARNS. And yours?

Mr. LOUNSBURY. My answer would be no as well.

Mr. STEARNS. If not, what is? In the first panel one person said yes and two said no, but I forgot to ask them what is. What is, Mr. Castro, that preempts this in your opinion?

Mr. CASTRO. The threat is the——

Mr. STEARNS. Could you have your mic on?

Mr. CASTRO. The threat is the remote access threat enabled by poor practices on the intended victims either not having adequate defense in-depth and protection of critical data, and also quite frankly increasingly folks are just succumbing to pfishing attacks that are very well constructed. But those pfishing attacks are the entry point for remote access attack attempting to acquire mostly intellectual property.

Mr. STEARNS. Not in the supply chain?

Mr. CASTRO. No, I would not put the supply chain in that.

Mr. STEARNS. OK, that's interesting. Mr. Lounsbury?

Mr. LOUNSBURY. I believe the supply chain is part of the problem. I think the actually immediate risk is from external attack, whether from outsiders or people who have been placed inside organizations.

Mr. STEARNS. So you are not worried about malware or all these other things, you are worried about somebody externally, either through pfishing or some kind of overt action getting in and then having the piece of software placed there?

Mr. LOUNSBURY. Malware is part of that problem. Malware takes advantage——

Mr. STEARNS. But you are not worried about the supply chain per se as you are worried about somebody overtly coming in?

Mr. LOUNSBURY. Supply chain encompasses many phases.

Mr. STEARNS. OK, it gets complicated. All right. Each member, what are the current supply chain practices and processes that could prevent or detect corrupt, compromise or counterfeit components in the supply chain? Mr. Castro?

Mr. CASTRO. Well, I mentioned the one that we observe most frequently with the clients that we support, and that is a very aggressive due diligence program, not quite frankly on every component that a company might buy but the identification of where the critical paths are, the tasks that lead to a company's crown jewels. And then ensuring that every component that might by compromised in that path has been vetted, not only in terms of the pedigree of the component but knowing who are the people responsible for servicing it and the other support structure around it.

Mr. STEARNS. Mr. Lounsbury?

Mr. LOUNSBURY. There are many steps in the development and furnishing of a product. And what we look at is the organizational best practices to make sure that a supplier is using the best practices during their processes throughout the supply chain to make sure that they are doing everything they can to prevent those vulnerabilities from being there so they can't be exploited later.

Mr. STEARNS. Who in the supply chain should ensure tighter chain of custody controls, Mr. Castro?

Mr. CASTRO. The question again is who in——

Mr. STEARNS. Who in the supply chain should ensure tighter chain of custody controls?

Mr. CASTRO. Well, again, I would just go back to the simple thing that we practice every day in each of our lives and that is buyer beware. If there is a purchasing order that's cut on behalf of an engineer and a company, then we would look to the engineer to make sure that it is to the best extent possible that they have been able to vet the pedigree of the product.

Mr. STEARNS. Mr. Lounsbury?

Mr. LOUNSBURY. I would concur with Mr. Castro. Each link in the chain has to look up to its suppliers and also downstream for its responsibility for the fulfillment, delivery, sustainment and eventual retirement of the products that it sells.

Mr. STEARNS. What can government do to create or incentivize the deployment of those additional capabilities that some of you folks would think is necessary? What can we do?

Mr. CASTRO. Well, again, going back to my testimony, I think the biggest thing that the government provides is information with regard to the source of potential threats and activity that's seen in this space. Again the Office of the National Counterintelligence Executive Program has been commended as exemplary in this case. They have a very vigorous outreach to industry to try to provide both at the classified level and to the unclassified level an understanding of where the problems are.

Mr. LOUNSBURY. Focusing on the ease of COTS ICT, the most important thing the government can do is in fact as said just a moment ago, is to make sure that it is using best practices when it does procurement to make sure that they have identified trusted technology partners.

Mr. STEARNS. My time has expired. The gentlelady from Colorado.

Ms. DEGETTE. Thank you, Mr. Chairman. As we continue our reliance, to increase our reliance on technology, we need to really look at all the implications of its use and include any vulnerabilities and threats presented by new technologies. So Mr. Castro, I wanted to ask you, do you think that the threats due to the new technologies are increasing in scope and sophistication?

Mr. CASTRO. I am sorry the threats are what?

Ms. DEGETTE. The threats due to the new technologies are increasing.

Mr. CASTRO. Oh, no question about it. An example would be smartphones and the applications that go on them. The application industry has just exploded. Some suppliers and some maintainers of application super supply stores do do some vetting, but quite frankly that is an area that we all should be concerned about as

we buy a very cheap app to put on our phone, but yes, I agree with you.

Ms. DEGETTE. Almost two-thirds of U.S. Firms report that they have been victims of cybersecurity incidents or information breaches. And as you allude to, the volume of malicious software on American networks has more than tripled since 2009. And so I am wondering in specific about the challenges the Federal Government faces in responding to those rapidly evolving threats.

Mr. CASTRO. Well, again the role of the government in my view is education. There's a tremendous amount of information that the government holds, both open source and classified, that should be made available to the private sector through properly vetted information channels.

Ms. DEGETTE. OK. Now James Clapper, who's the Director of National Intelligence, was talking to the Senate committee about a year ago and he talked about a new phenomenon known as convergence. Are you familiar, Mr. Castro, with network convergence?

Mr. CASTRO. Yes, ma'am.

Ms. DEGETTE. And can you talk about what that is?

Mr. CASTRO. Well, I think in terms that we would understand it is where we rely upon each of the devices in an integrated way.

Ms. DEGETTE. Right.

Mr. CASTRO. So it may be that your BlackBerry might be linked or synched to your home personal PC or to your laptop. So the problem there is a vulnerability in one part of that chain is easily introduced into the other part.

Ms. DEGETTE. Into the other parts. So it is because video, data, voice, everything are all converging on one common network, and that's part of this new technology that has developed that you talk about like with the iPhones and things like that, right?

Mr. CASTRO. Right.

Ms. DEGETTE. And I am wondering if both of you could talk about the risks of that type of convergence technology, the increased vulnerabilities if they are put into cyberterrorist hands.

Mr. CASTRO. Briefly, although I will be repeating myself a little bit. But an example would be if you bought an app for whatever smartphone, mobile device you have that is corrupted, it is quite possible that that can be the front door that allows someone to have access to your own home personal machine where you might have some more sensitive data stored or you might have the keys to being able to get to your financial accounts and things of that nature.

Ms. DEGETTE. And that can be extrapolated to problems on the government networks, too, right?

Mr. CASTRO. Well, yes, but fortunately in most places in the government this whole notion of how to deal with mobile devices is undergoing quite a bit of scrutiny. Policies are being adopted that would provide some partitioning between mobile users and the enterprise that they support.

Ms. DEGETTE. Well, I am thinking about—- I am glad they are putting policies into place, but I am thinking about like if there's a National Lab and there's a smart device being used to collect and process information for research at a National Lab, if somebody was able to get in there, that could cause significant harm, correct?

Mr. CASTRO. Well, there is some potential for that, but since you talk about the National Labs, I will tell you that in my time and experience in government that they are some of the most very, very far in front, as Gil mentioned, with regard to constructing the kind of policies and actual hardware limitations to prevent that, particularly in dealing with some of the more sensitive things that the labs do.

Ms. DEGETTE. That's good to know.

Mr. CASTRO. But it's a point very well taken, the threat of mobile devices is one that has really mushroomed onto the landscape and it is one that we are all scrambling to find the right balance between providing the individual user the flexibility that the mobile device provides but also protecting the integrity of our data.

Ms. DEGETTE. Mr. Lounsbury, do you want to comment on that briefly?

Mr. LOUNSBURY. I think there are a couple of comments. First, the issue about the growth and capabilities of computer systems and networks is a coin with two sides. Of course the increase in complexity does come with an increase in vulnerability, yet it also adds the ability of the additional processing power and the additional awareness of what is going on to actually recognize attacks and proactively create defenses. I.

I concur with the issue of convergence, sometimes we hear it called as, you know, bring your own device where there are new devices coming in that may bring their own vulnerabilities. And so this is why it is in fact essential to have not only policies of course beyond the supply chain but also in the supply chain to make sure that those devices that are coming in have undergone the scrutiny and correct practices to make sure that they are safe.

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

Mr. STEARNS. The gentlelady's time has expired. The gentleman from Nebraska, Mr. Terry, is recognized for 5 minutes.

Mr. TERRY. Thank you, Mr. Chairman. And you're here as a different perspective from the first panel, kind of non-governmental perspective. And so I kind of want to follow through with your unique position here for today's hearing. And we heard the gentleman from GAO talk about unauthorized materials or whatever, computers, devices. And I want to work through that because I am still very concerned about how loose the authorizations may be. It seems to me the best practice that's being recommended here for any, for Department of Defense or DOE or whatever government agency that is dealing with critical issues is that they should only be allowed to purchase from an authorized vendor, of which evidently the vendor then has certified everything back, that they can then trust the individual parts, whether it is software, chips, hardware, have not been compromised in any way. So my question to you is, is that a best practice? Do we need to add more definition to it? And do we need further authorizations down the supply line? Mr. Castro and then Mr. Lounsbury.

Mr. LOUNSBURY. I guess, if I may start, I would concur with what you say there. Ultimately people, use of COTS implies that an agency, in this case a government agency, purchases from a commercial marketplace. And so the question is what are the standards that your supplier uses to demonstrate that they can be

trusted. Part of that would be the processes they have for themselves throughout their product development and fulfillment lifecycle, but also are they imposing those standards on those suppliers as well? You think about first you design a product, then you get sources for components, those components have to undergo the same standards or be held to the same standards that you would hold yourself to as a trusted vendor.

Mr. TERRY. And do you think that is sufficient, that they just—I don't have the confidence that the supplier actually has any level of control in India or China or manufacturing facilities. How do they have a level of surety that something's not being compromised way down the assembly line?

Mr. LOUNSBURY. In the commercial world typically we look to some sort of a conformance program where a supplier would submit evidence, either through a third-party lab and certainly to an independent certification authority, to make sure that they have in fact given some evidence of those best practices before they are, you know, recognized as a trusted partner. And then, yes, there is the burden of everybody in the supply chain for making sure that their partners are trusted. It is a very, you know, fast branching supply chain, and it is really—you have to pick a scalable way of doing that.

Mr. TERRY. Mr. Castro, do you have anything to add?

Mr. CASTRO. I would offer quite frankly, and this may be out of skew with the thrust of your question but I can't diverse my 44 years in government service either. I think this has to be approached with a really sensible sense of scale and scope, in that you are not going to test every resistor that goes into every motherboard of every computer. And I think the DOD program is exemplary in this in that they have started, they have prioritized those systems that they believe should have this extra scrutiny.

The other thing that the customer can always do, that is to say the person at the end, is you pick every fifth Dell computer that comes out of the box and you really run it through its paces to the greatest extent you can. And there are folks who are very, very good at that, including looking for signs of tampering and things of that nature. So some random—I said every fifth, but it would be a random sampling of the devices that you get, but the point being that unless you are willing to authorize extraordinary amounts of money in this area it has to be done with some reasonable balance involved.

Mr. TERRY. Thank you.

Mr. STEARNS. I thank the gentleman. The gentleman from Georgia, Mr. Gingrey, is recognized for 5 minutes.

Mr. GINGREY. Mr. Chairman, thank you. Mr. Lounsbury, how can the government and the private sector benefit from a public-private partnership in developing international standards?

Mr. LOUNSBURY. I think there are a couple of ways that that can happen. First, the government quite often brings a unique set of needs and perspectives and set of requirements to the party. And of course, on the other hand, any provider who values their reputation wants to make sure that their products will meet those needs so they can frankly sell into that sector. Of course they have do it

in a way that still keeps them in a commercial business. So there's that match of buyer need and supplier response.

The other part is we have to recognize then, as we have heard many times, the supply chain is global. It says on some of our devices designed in California, made in China. Right? And so these have to be international standards so that the bar can be raised on a global basis so that if you know that you have seen a trusted technology provider here, and I do want to emphasize that when we look at this we talk about the organization, not a specific product. So we look at is that organization following these best practices in a verifiable and certified way. And you can look——

Mr. GINGREY. Well, let me interrupt you just for a second because of the limitation of my time and I will cut right to the chase. More importantly, how do you envision other countries implementing the international standards of the Open Group?

Mr. LOUNSBURY. The Open Group—first we—our standards are principally commercial standards. These are ones where companies voluntarily comply with them and enter into certification programs. We do, however, have liaison with ISO, the international standards body and specifically the working group within ISO that will take these standards and make them international. We are very active in making sure that that happens. So they are both de facto standards that can be adopted by industry and de jure standards that can be implemented by——

Mr. GINGREY. If standards such as these are implemented internationally, should the United States refuse to do business with countries that don't implement those standards?

Mr. LOUNSBURY. I think that when the United States procures things they should procure from suppliers that have taken the time to do the job right by following the international standards.

Mr. GINGREY. Thank you. Mr. Castro, the current approach to IT supply chain risk is a patchwork of varying policies and procedures that are not coordinated across the government. What can be done to facilitate a coordinated approach that reasonably and adequately addresses the risk while avoiding excessive cost, burdensome regulation or marginal results?

Mr. CASTRO. That's a tough one, Congressman. I think it begins with the fact that my sense from where I sit is that within the government there has been a very, very succinct wakeup call. It is evidenced in the testimony that General Clapper and others have provided to you and other committees.

The other thing is that it is increasingly becoming threat based, and that was part of the essence of my oral statement, is that we simply can't go down every road, but we know where there are two very big roads that we have to watch. But clearly all the things that you asked for in that question represent the Nirvana at the end of the process. I am not sure we are anywhere close.

Mr. GINGREY. Let me follow up on that with this. For example, the GAO report, it highlighted deficiencies of DOE, DHS, DOJ, I am sorry, Department of Justice, and rightly recommends corrective action. Their recommendations for executive action is directed at each department individually, if I understand the report.

How should the government coordinate this solution for the entire Federal Government?

Mr. CASTRO. Well, again I think that the way the Federal Government is organized that there's no doubt somebody in OMB who has this in their portfolio to coordinate across, but the other thing I think that's recognized in the report is that one size does not fit all. As the committee members have already pointed out, you have concerns about DOE because they have such a critical part of not only our national security structure, but our energy provision structure. The report also singled out DHS, but quite frankly DHS is not a big component in terms of driving the IT enterprise.

Mr. GINGREY. Well, let me real quickly because my time is running out, I really respect the fact that you have got 44 years of experience at the Federal level, but, you know, it would seem to me that lack of coordination would be more advantageous let's say to a company like the one that you currently work for, the Chertoff Group, whereas from the Federal Government perspective coordination would be better, more coordination. So where do you draw the line in regard to that?

Mr. CASTRO. Well, again I think it is a balance. You want—there definitely needs to be a common set of standards, a common set of government regulations that OMB would administer and see just like they do FISMA and report in the same way as FISMA compliance is reported, but I think also that Mr. Vega at DOE has a set of problems, the DOD program has a different set of problems. As long as they meet the common standard then they can in their directions.

Mr. GINGREY. OK, thank you. Thank you both and thank you, Mr. Chairman.

Mr. STEARNS. I thank you. The gentleman from Virginia is recognized for 5 minutes.

Mr. GRIFFITH. I don't think I will take the whole 5 minutes, so if anybody else has other questions I would be happy to yield. But I do have one. I have been listening to the testimony and bringing myself a little education on this, which I like coming to these hearings. Thank you, Mr. Chairman, for holding it.

You indicated, Mr. Castro, that one of the things we need to do is have the Department of Defense working with private industry and I agree with that. But my question is at what point do they step in? And do they need to be taking an active role in defending our private industries? Here is the dilemma I've got. In World War II the Allies broke the German code, they had to make some very tough choices and history looks back on some of the choices very critically. But they had to make some tough choices because they knew some things the Germans were doing, but they knew if they stopped it there might be the possibility that the Germans would figure out that they had broken the code and then that would endanger all kinds of other operations. So now we are faced in a slightly different situation. If the defense folks know that somebody is stealing our private information because they have tapped into it by their defensive measures in trying to protect our national security on the defense side, how do they work out balancing that out? And how do they tip off or do they just take measures on behalf of the private industry to defend our economic system without tipping off X, Y, Z country that we are on to them? That's the basic gist of my question. If you could help me on that.

Mr. CASTRO. OK, very well founded. The difference where the analogy isn't quite possibly in synch is that the time frame that we are operating with regard to the breaking of Ultra and things like that you refer to in World War II, we had a much greater time frame, duty cycle. Today it moves much, much more quickly and therefore I do come very much into the direction that your question was going and that there needs to be greater transparency between what the intelligence community within the DOD sees and making that information available to the private sector. And again very, very—I think well spoken is the fact that there are bills before the House, particularly the one out of the HPSCI, the Rogers-Ruppersberger bill, that does attempt to address that issue and put quite frankly the DOD intelligence assets into the game, properly supporting through the DHS front door the private industry. So your analogy is very, very well taken and I understand and totally agree.

Mr. GRIFFITH. Thank you very much. Mr. Chairman, unless somebody wants me to yield time to them, I would yield back.

Mr. STEARNS. The gentleman yields his time back, and I will ask two questions and the gentlelady is welcome to offer her questions. A question for both of you, who should be the innovator in this place in developing a common criteria network; should it be the government or the private sector?

Mr. LOUNSBURY. Mr. Chairman, I actually believe that the public sector does need to lead in this area.

Mr. STEARNS. The government should.

Mr. LOUNSBURY. Pardon me, excuse me, the commercial sector. Sorry to be unclear.

Mr. STEARNS. The commercial sector, OK, and you, Mr. Castro?

Mr. CASTRO. I would agree.

Mr. STEARNS. OK are there advantages basically because the private sector is more innovative?

Mr. LOUNSBURY. I think it is a question——

Mr. STEARNS. It is closer to their bailiwick?

Mr. LOUNSBURY. I think it is a question of market pressure, sir. I think the pace of innovation forces them to respond very quickly, and frankly they need to innovate and respond at the speed that is driven by the market and by the emerging threats.

Mr. STEARNS. Mr. Castro, do you agree?

Mr. CASTRO. I agree.

Mr. STEARNS. Mr. Castro, if one begins from the premise that a supply chain vulnerability has already been exploited and currently exists within an IT enterprise, what should a supplier or that matter an agency do to mitigate this risk?

Mr. CASTRO. OK, well, this in fact is the topic of the moment. It is called presumption of breach or operating under attack.

Mr. STEARNS. Presumption of——

Mr. CASTRO. That your system has been breached and that's the way you go about constructing the defense.

Mr. STEARNS. OK.

Mr. CASTRO. DOD put out their strategy for operating in cyberspace last summer. That is at the heart of it. What you then have to do, however, is to say if in fact the assumption is that the adversary is in my system, I need to identify very, very precisely what

are my crown jewels that I hold in that system and I need to protect those to the maximum extent possible and I need to make sure that those who have authorization to be able to access those crown jewels, that their activity is very, very well accounted for. We call that data centric defense.

Mr. STEARNS. Mr. Lounsbury, you might want to comment on what Mr. Castro said.

Mr. LOUNSBURY. Thank you. I would agree with the spirit of what Mr. Castro says, but I think one of the essential pieces of this is that you make the best practices commonplace. I think that everybody understands that there are issues about how you do security development and engineering, things like threat analysis, threat mitigation, how you respond to those threat analysis through a design, one-time protection techniques, vulnerability analysis, all those tings in the development phase, and then you actually must extend them to the supply chain, but it can't be treated as a product by product activity. It has to be something you internalize to your company's processes in order to not have to do it every single time, that you can look to a provider and say yes, we can deal with them and know their products are trustworthy.

Mr. STEARNS. All right, thank you, Ms. DeGette.

All right, at this point, it appears our questions for the second panel are complete.

I want to thank the witnesses for coming today and for their testimony and members for their devotion to this hearing. The committee's rules provide that members have 10 days to submit additional questions for the record to the witnesses.

And, with that, the subcommittee is adjourned. Thank you.

[Whereupon, at 12:02 p.m., the subcommittee was adjourned.]

○