

From: [NPPD OPA](#)
Subject: NPPD VISION: March 22, 2016 - Under Secretary Spaulding Shares NPPD Transition Report with Employees
Date: Tuesday, March 22, 2016 5:17:46 PM
Attachments: [image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[image006.png](#)
[image007.png](#)
[image008.png](#)
[image009.png](#)
[image010.png](#)
[image011.png](#)



March 22, 2016

In This Issue:

NPPD AT WORK

[Under Secretary Spaulding Shares NPPD Transition Report with Employees](#)

[NPPD Leadership Present Awards to Federal Protective Service Employees](#)

[Danny Toler Added to CS&C Leadership Team](#)

[NPPD Employee Recognition Awards Ceremony Postponed](#)

[Secretary Johnson Certifies Cyber Automated Indicator Sharing Capability](#)

[Secretary Johnson Goes Undercover on the NCCIC Floor](#)

[Office of Cyber and Infrastructure Analysis Employees Receive First OCIA Awards](#)

[OBIM Employee Participates in Deputy Secretary's New Orleans Town Hall Meeting](#)

[NPPD Privacy Office to Host Trainings in National Capital Region](#)

[Employees with Travel Cards must Update Information in JP Morgan's PaymentNet](#)

I think that we need an agency, not just a directorate. We need an agency focused on cybersecurity and infrastructure protection.

And so our vision is to reform, rebuild NPPD, which is a directorate, into a cyber and infrastructure protection agency. Given our current threats to cyber, to critical infrastructure, I think we need an agency that is focused on this.

I want see this DHS component with more of an operational focus in an agency like TSA, the Coast Guard, CBP and ICE.

Certainly the cybersecurity mission of the federal government warrants that.

-- Secretary Jeh Johnson
Testimony to the Committee on
Homeland Security, March 16, 2016

[Help Your NPPD Colleague by Donating Leave](#)

[Welcome Aboard](#)

[Out and About](#)

NPPD EMPLOYEE DEVELOPMENT AND WELLNESS RESOURCES

[Detail Opportunities](#)

[Treasury Executive Institute - Cornell Leadership Certificate Program Accepting Applications](#)

[NPPD Jobs](#)

DHS

[Cyber Storm V: Testing the Nation's Ability to Respond to Significant Cyber Incidents](#)

[Avoiding Online Fraud Takes More than Luck](#)

TIP OF THE WEEK

[Enjoy the Cherry Blossoms](#)

NPPD AT WORK

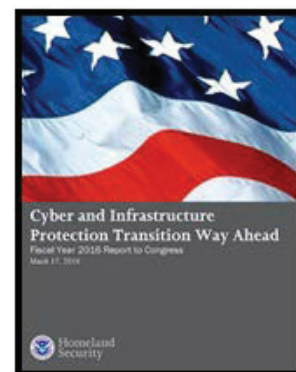
Under Secretary Spaulding Shares NPPD Transition Report with Employees

The following message was sent to NPPD employees on March 18, 2016

Dear Colleagues:

Our component continues toward becoming Cyber and Infrastructure Protection (CIP) through our Transition planning efforts. As some of you know, NPPD transmitted a report to the Office of Management and Budget that provides additional information about the Department's plan to evolve NPPD to CIP.

This report has now been approved for transmittal to Congress, with whom we are working on legislation to authorize key elements. This report is entitled Cyber and Infrastructure Protection Transition Way Ahead, and contains specifics regarding the organization and additional capabilities of the new CIP structure and further information about the benefits of these changes. This report has been posted on the [Transition Connect](#) site. I encourage you to read the report and to ask questions and provide your feedback.



"I think that we need an agency, not just a directorate. We need an agency focused on cybersecurity and infrastructure protection."

"And so our vision is to reform, rebuild NPPD, which is a directorate, into a cyber and infrastructure protection agency. Given our current threats to cyber, to critical infrastructure, I think we need an agency that is focused on this."

"I want to see this DHS component with more of an operational focus in an agency like TSA, the Coast Guard, CBP and ICE."

"Certainly the cybersecurity mission of the federal government warrants that."

--Secretary Jeh Johnson
Testimony to the Committee on Homeland Security,
March 16, 2016

This report contains more detailed information about the envisioned structure at CIP's Final Operating Capability, and outlines some significant but necessary changes in order to improve our component's effectiveness. I want to reiterate that the plans in this report are plans, and represent the deliberations of our Champions, Senior Accountable Officials, and the members of their working groups.

The overwhelming majority of employees will not be affected by the forecasted changes. If you are affected however, we will be reaching out to you with more details and to answer any questions that you may have. I recognize that change is inherently stressful, and I am aware of the considerable time and effort that you all have given in support of this important effort.

In the meantime, I encourage all employees to reach out to their Champions or SAOs with their questions and concerns, or to send their comments and inquiries to the JoinUs@hq.dhs.gov inbox.

Best,

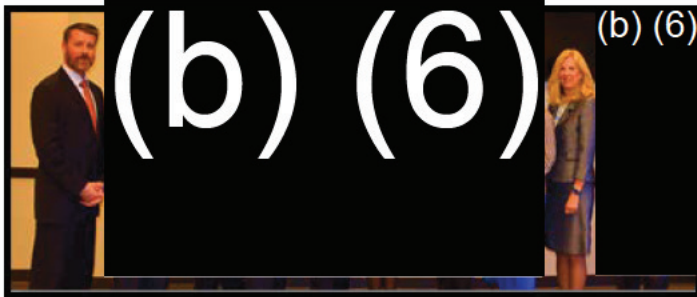
Suzanne Spaulding
Under Secretary



NPPD Leadership Present Awards to Federal Protective Service Employees

By (b) (6), Office of External Affairs, Federal Protective Service

The National Protection and Programs Directorate (NPPD) hosted a ceremony in Rosslyn, Va., March 16, 2016, to present awards to Federal Protective Service (FPS) employees who traveled to town for the NPPD Annual Award Ceremony that was unexpectedly postponed due to the Metrorail



NPPD Leadership present Employee Recognition Awards to FPS employees.

The ceremony recognized the extraordinary accomplishments of FPS employees during 2015. FPS Awardees honored during the ceremony include:

- (b) (6), Region 7 – Teamwork Award Winner
- (b) (6), Region 4 – Agility Award Winner
- (b) (6), Region 1 – Agility Award Winner
- (b) (6), Region 1 – Innovation Award Team Winner (representing team members (b) (6))

shut down. The [annual awards program](#) recognizes NPPD employees' outstanding achievements in seven categories such as Agility, Emerging Leader, Innovation, Leadership, Teamwork, Valor, and the Under Secretary's Mission Excellence Award.

The ceremony recognized the

- (b) (6), Region 4 – Leadership Award Winner
- (b) (6), Region 9 – Leadership Award Winner
- (b) (6), Region 9 – Leadership Award Winner

Leadership participants include Under Secretary Suzanne Spaulding, Deputy Under Secretary Ronald Clark, Deputy Chief of Staff Patricia Weichmann-Morris, FPS Director L. Eric Patterson, FPS Deputy Director for Operations Richard Cline, FPS Deputy Director for Training and Professional Development Richard Swengros, and Acting Chief of Staff (b) (6), (b) (7)(E).

Under Secretary Spaulding praised the honorees for their agility, valor and commitment to excellence in support of the NPPD mission.



Danny Toler Added to CS&C Leadership Team

The following message was sent to employees on March 18, 2016

Dear Colleagues:

I'm writing to share news of an important addition to the CS&C leadership team. On March 21, Danny Toler, current Director of Network Security Deployment (NSD), will become one of CS&C's Deputy Assistant Secretaries.

Over the course of almost four years at CS&C, Danny has become a widely respected and trusted leader who epitomizes professionalism and integrity. Danny came to NPPD following his extensive experience in network architecture at the Department of State and, before that, the U.S. Information Agency. While serving on active duty in the United States Air Force, he was a systems analyst at Randolph AFB, San Antonio, Texas. Mr. Toler received a B.S. in Business Administration with an emphasis in Computer Information Systems from Charleston Southern University.

I'm happy to say that (b) (6), current NSD Branch Chief for Systems Engineering and Acquisition, will take over as Acting Director of NSD once Danny begins his new position.

Please join me in congratulating Danny on his new position and in providing him with your full support as we all work together to advance our vital mission of strengthening the security and resilience of the nation's critical infrastructure.

Sincerely,

Suzanne Spaulding
NPPD Under Secretary



NPPD Employee Recognition Awards Ceremony Postponed

By (b) (6), NPPD Office of Public Affairs

NPPD's annual Employee Recognition Awards Ceremony scheduled for March 16 was postponed until early April due to the unexpected closure of the Washington, D.C. Metro transit system for emergency inspections of the system following an early morning tunnel fire March 14.

Federal workers in the National Capital Region had the option to take unscheduled leave or telecommute because of the outage.

"We are disappointed that we had to postpone the awards ceremony," said Under Secretary Spaulding, "but given the number of employees who rely on the metro system to travel to and from work we made the decision to ensure as many employees from across the region were able to travel to the ceremony."

Employees will be notified of the new date and time as soon as possible. Please direct any questions regarding the NPPD Employee Recognition Awards to (b) (6), Director of Employee Engagement, at (b) (6)



Secretary Johnson Certifies Cyber Automated Indicator Sharing Capability

By (b) (6), Office of External Affairs, Office of Cybersecurity and Communications

Secretary Jeh Johnson visited the [National Cybersecurity and Communications Integration Center \(NCCIC\)](#) on March 17, 2016, and announced that DHS has successfully deployed a system to enable the timely exchange of cyber threat indicators among federal departments and agencies and private sector entities, as required by the Cybersecurity Act of 2015.

"Through our [Automated Indicator Sharing](#), the NCCIC will facilitate the sharing of cyber threat indicators between the government and private sector at machine speed," Johnson said, "which will allow participants to mitigate cyber threats in real-time, ultimately reducing the prevalence of cybersecurity compromises."



CS&C Assistant Secretary Andy Ozment and Under Secretary Suzanne Spaulding brief members of Congress on the NCCIC floor with Secretary Jeh Johnson (DHS Photo by (b) (6)).

Rep. Michael McCaul (R-TX), Chairman of the House Committee on Homeland Security joined Secretary Johnson at the certification event. The Secretary thanked Congress for passing the Cybersecurity Act of 2015, which established the NCCIC as the Federal government's hub for cyber threat indicator sharing.



Secretary Jeh Johnson briefs members of Congress inside the NCCIC (DHS Photo (b) (6))

As the [Secretary described in his remarks](#), the AIS capability is comprised of three key elements:

- Technology at the NCCIC that manages AIS;
- Technology at each participant's location that allows them to send and receive indicators with the NCCIC; and
- Processes at the NCCIC for analyzing those indicators

to mitigate privacy risks and to use those indicators, in association with other tools like EINSTEIN, to detect cyber threats impacting federal networks.

Importantly, the Cybersecurity Act of 2015 also provides targeted liability protection to companies that share cyber threat indicators with DHS or with each other.

Privacy was a key priority when developing this system. DHS is committed to minimizing the privacy impacts of indicator sharing by screening all cyber threat indicators received for issues with privacy and civil liberty.

"Moving forward, this system will serve as the 'See Something, Say Something' of the Internet," said Johnson. "When one participant detects a threat, all participants will learn about it."

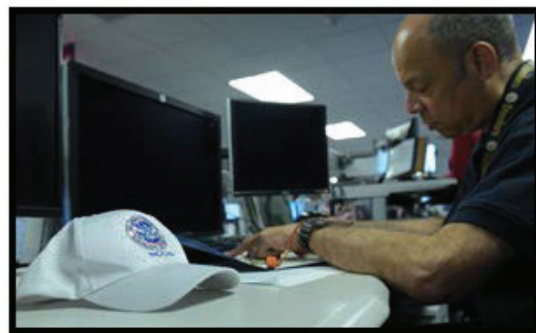


Secretary Johnson Goes Undercover on the NCCIC Floor

By **(b) (6)**, *Office of External Affairs, Office of Cybersecurity and Communications*

If you had strolled through the [National Cybersecurity and Communications Integration Center \(NCCIC\)](#) on March 11, 2016, you probably would have done a double-take as you passed the duty officer station. Standing at that desk, conducting the afternoon's watch activities in cybersecurity-casual attire, was none other than Secretary of Homeland Security Jeh Johnson, "Undercover Boss" style.

Secretary Johnson spent much of the afternoon at the NCCIC, familiarizing himself with the organization and learning about its different components, activities, and functions. Prior to standing in at the Duty Officer station, Secretary Johnson chatted with NCCIC watch members and discussed cybersecurity roles and responsibilities. He also shadowed the National Cybersecurity Assessment and Technical Services (NCATS) team and received a briefing from the team on their mission and services, which includes independent, third party review of risk, vulnerabilities, and cyber hygiene. He also received a short demonstration on how NCATS executes these capabilities.



Secretary Johnson on the NCCIC floor (DHS photo by (b) (6)).

Secretary Johnson also got the chance to



Secretary Johnson addresses employees on the NCCIC floor (DHS photo by (b) (6)).

express his appreciation to the teams. He presented multiple letters of appreciation, commending NCCIC staff for the important work they are doing in support of the Department's cybersecurity efforts.

Secretary Johnson also spoke to some information security students touring the NCCIC from the University of Pittsburgh as part of the college's ["Shadow in Your City" program](#), which is designed to provide groups of students with exposure and knowledge of a company or organization that they are interested in working for in the future.

The secretary concluded his visit at the NCCIC Senior Watch Officer's desk, finishing staff work while observing the NCCIC operations on a late Friday afternoon.



Office of Cyber and Infrastructure Analysis Employees Receive First OCIA Awards

By (b) (6), Office of External Affairs, Office of Cyber and Infrastructure Analysis

Office of Cyber and Infrastructure Analysis (OCIA) Director Brandon Wales presented the inaugural [OCIA Director's Awards](#) to employees on February 2, 2016, to recognize outstanding work conducted in 2015. Awards were given to individuals and groups in four categories: Excellence, Innovation, Collaboration, and Boldness. Nominations were submitted by OCIA peers and selected by an Awards Board.

"I'm extremely proud of all of our OCIA personnel for the important work they are doing to strengthen our analysis," said Wales. "Our focus on innovation and collaboration is impacting key decisions affecting the security and resilience of the Nation's critical infrastructure."

- (b) (6) – 2015 Director's Award for Excellence
- (b) (6) – 2015 Director's Award for Innovation
- (b) (6) – 2015 Director's Award for Innovation
- (b) (6) – 2015 Director's Award for Boldness
- Integrated Analysis Cell: (b) (6) – 2015 Director's Award for Boldness
- Intelligence Support Branch: (b) (6) – 2015 Director's Award for Collaboration
- Strategic Studies Team: (b) (6) – 2015 Director's Award for Collaboration



OBIM Employee Participates in Deputy Secretary's New Orleans Town Hall

Meeting

By (b) (6), *Internal Communications Specialist, Office of Biometric Identity Management*

In an effort to acknowledge the hard work and dedication of the Department of Homeland Security (DHS) personnel, Deputy Secretary Alejandro Mayorkas has been traveling around the United States to hold “Meet and Greet” sessions with employees. Most recently, Mayorkas participated in a Town Hall meeting on February 26, 2016, in New Orleans, where he highlighted employee service and support to the Department. (b) (6), who is with NPPD’s Office of Biometric Identity Management (OBIM), was selected to participate.

Since May 2010, (b) (6) has worked as an Information Technology Manager in OBIM’s Identity Operations Division in the Systems Operations and Maintenance Branch in the DHS Data Center One in Stennis, Mississippi. His primary duties include managing hardware and overseeing a contracting staff. This was (b) (6) first Town Hall and he was excited to hear first-hand from Department leadership.

Deputy Secretary Mayorkas talked about NPPD as the leader of DHS Cyber Security. “He reinforced this message to all of us, that all of NPPD has an important role in DHS,” said (b) (6)

Mayorkas also discussed the roles of other agencies within DHS, such as U.S. Custom and Border Protection and the U.S. Coast Guard. He emphasized the importance of dealing with the issues of hackers. Reflecting on his Town Hall participation, (b) (6) expressed his gratitude for the opportunity to meet and talk with the Deputy Secretary. In fact (b) (6) was surprised to hear that both he and Mayorkas had a similar background and mindset stating, “he came from humble beginnings and is proud of our country and his job, like me.” Further noting that he and Deputy Secretary Mayorkas “both believe in the core mission of DHS which is to keep America safe from the many threats we face.”

(b) (6) said he now has a better understanding of the connection amongst the subcomponents of NPPD and their relationship within the Department. He said it was a great opportunity to network with other colleagues in the Department.



Employees with Travel Cards must Update Information in JP Morgan’s PaymentNet

By (b) (6), *Budget, Finance and Acquisition, Office of Cybersecurity and Communications*

Employees who are issued a government travel credit card, also known as an Individually Billed Account (IBA) need to ensure their billing information consistent in both Concur Government Edition profile (CGE) and [PaymentNet](#) because these two systems are not connected. Government credit cards are issued by JP Morgan, PaymentNet, is the online system that stores the cardholders’ billing information.

If the traveler’s information is not properly updated in PaymentNet the credit card will be returned as undeliverable. Government cardholders can only update their billing information by sending an email with their updated information to nppdtravelcard@hq.dhs.gov.

For travelers with an IBA government travel card, please ensure all billing information is accurate and up-to-date in PaymentNet, particularly if a new JP Morgan card will be or was recently issued. Expiring cards are reissued six weeks before the end of the expiration month and year listed on the card.

Employees are encouraged to reach out to nppdtravelcard@hq.dhs.gov with any additional questions.



NPPD Privacy Office to Host Trainings in National Capital Region

By **(b) (6)**, *Director, NPPD Office of Privacy*

NPPD's Office of Privacy will be hosting Privacy Training Day events on March 29, March 30 and March 31, 2016. Employees and contractors in the National Capital Region can choose to participate from multiple NPPD locations.

The course objectives are to:

- Learn how to define privacy in the context of government records
- Be able to identify personally identifiable information (PII)
- Be familiar with the DHS privacy framework
- Understand the DHS Fair Information Practice Principles (FIPPs) and how they apply to you
- Learn how to recognize, avoid, and respond to privacy incidents

Dates and Locations:

- Tuesday, March 29, 8:30 – 9:30 a.m.
800 N. Capitol St., FPS 3rd floor RMD Conference Room
- Wednesday, March 30, 9 – 10 a.m.
1616 N. Fort Myer Dr., Room 1890 (Rosslyn)
- Wednesday, March 30 1:30 – 2:30 p.m.
1310 N. Courthouse Rd., Room 05-360 (Courthouse)
- Thursday, March 31 1 – 2 p.m.
1110 N. Glebe Rd., Room 1128 (Glebe)

Employees who have not fulfilled their annual privacy training requirement will receive full credit for attending this training in PALMS. Advanced registration in PALMS is required, contact NPPDPrivacy@hq.dhs.gov for instructions.

Please email NPPDPrivacy@hq.dhs.gov to register, and include in the body of your email which session you will be attending.



Help Your NPPD Colleague by Donating Leave

The following NPPD employees are experiencing a personal medical emergency and are eligible to receive donations through the Voluntary Leave Transfer Program (VLTP). If you would like to donate annual leave, please complete the [fillable PDF form](#), indicating the employee as the recipient, save the form and return it as an

attachment to save the form and return it as an attachment to (b) (6) @hq.dhs.gov and type VLTP Donation in the subject line of the message. Your email verification will be used in lieu of a hand signature.

- (b) (6), Management and Program Analyst, Office of Cybersecurity & Communications
- (b) (6), Management and Program Analyst, Office of Biometric Identity Management
- (b) (6), Physical Security Specialist, Federal Protective Service
- (b) (6), Contracting and Acquisition Advisor, Federal Protective Service
- (b) (6), Program Analyst, Office of Infrastructure Protection
- (b) (6), Human Resource Specialist, Federal Protective Service



Welcome Aboard

Federal Protective Service

- (b) (6), New Haven, Conn.
- (b) (6), Washington, D.C.
- (b) (6), Gulfport, Miss.

Office of Cybersecurity & Communications

- (b) (6), Pensacola, Fla.
- (b) (6), Pensacola, Fla.
- (b) (6), Arlington, Va.
- (b) (6), Arlington, Va.
- (b) (6), Arlington, Va.
- (b) (6), Pensacola, Fla.

Office of Infrastructure Protection

- (b) (6), Houston, Texas
- (b) (6), Arlington, Va.
- (b) (6), Arlington, Va.

Office of Cyber and Infrastructure Analysis

- (b) (6), Arlington, Va.
- (b) (6), Arlington, Va.
- (b) (6), Arlington, Va.

Office of Biometric Identity Management

- (b) (6), Arlington, Va.



Out and About

March 21

- **(b) (6)**, Deputy Director, Office of Emergency Communications, Office of Cybersecurity and Communications, will participate in a panel discussion entitled "Role of Statewide Interoperability Coordinators" at the International Wireless Communications Expo event in Las Vegas, Nev.

March 22

- **(b) (6)**, Deputy Director, and **(b) (6)**, Security Manager, Office of Emergency Communications, Office of Cybersecurity and Communications will participate in a panel discussion entitled "P25 Interoperability and System Update" at the International Wireless Communications Expo event in Las Vegas, Nev.
- **Bob Kolasky**, Deputy Assistant Secretary, Office of Infrastructure Protection will deliver remarks on requirements to protect critical electrical infrastructure at the 2016 Power Grid Resilience event in Philadelphia, Pa.
- **(b) (6)**, Director, Office of Cybersecurity and Communications will participate in a panel discussion entitled "How to Create a Cybersecurity Resilient Organization through Acquisition Changes" at the American Council for Technology - Industry Advisory Council Acquisition Excellence event in Washington, D.C.

March 23

- **(b) (6)**, Partnerships Branch Chief, Office of Cybersecurity and Communications, will participate in a panel discussion entitled "Improving Interoperable Communications" at the International Wireless Communications Expo event in Las Vegas, Nev.
- **(b) (6)**, Deputy Director, Office of Emergency Communications, Office of Cybersecurity and Communications, will participate in a panel discussion entitled "Early Builders of FirstNET-Ready LTE Networks" at the International Wireless Communications Expo event in Las Vegas, Nev.

March 24

- **Suzanne Spaulding**, Under Secretary will deliver a keynote address at the First National Conference of Minority Cybersecurity Professionals, hosted by the International Consortium of Minority Cybersecurity Professionals in Washington, D.C.
- **Andy Ozment**, Assistant Secretary will deliver remarks on cybersecurity act and protecting federal networks at the Information Security and Privacy Advisory Board Public Meeting in Washington, D.C.
- **Robert Kolasky**, Deputy Assistant Secretary, **(b) (6)**, Director, **Brandon Wales**, Director, Office of Infrastructure Protection, will speak at a forum on "Infrastructure Resilience and Mission Assurance: Fostering Civil/Military Collaboration for National Security" in Virginia Beach, Va.
- **(b) (6)**, Deputy Director, Office of Emergency Communications, Office of Cybersecurity and Communications, will deliver an overview of OEC at the International Wireless Communications Expo event Las Vegas, Nev.
- **(b) (6)**, Security Manager, Office of Emergency Communications, Office of Cybersecurity and Communications, will participate in a panel discussion entitled "An Update on the Project 25 Compliance

Assessment Program” at the International Wireless Communications Expo event in Las Vegas, Nev.

- (b) (6), Program Lead, Cybersecurity Education and Awareness, Office of Cybersecurity and Communications, will deliver remarks on cybersecurity education at the Coastal Virginia Cyber Symposium in Virginia Beach, Va.

March 25

- (b) (6), Program Analyst, Office of Emergency Communications, Office of Cybersecurity and Communications, will deliver an overview of OEC grant guidance at the International Wireless Communications Expo event in Las Vegas, Nev.



NPPD EMPLOYEE DEVELOPMENT AND WELLNESS RESOURCES

Detail Opportunities

NPPD Office of External Affairs Task Force

NPPD’s Office of External Affairs has multiple detail positions for employees at the GS-12 and above level, to serve as part of a Task Force that will be responsible for developing the processes, tools, and best practices for an enterprise-wide, component-level External Affairs (EA) Office at NPPD.

These positions will be instrumental in building a foundational structure of External Affairs. The selected employees must excel at building processes and demonstrating productive results and have an understanding of or experience working with offices of public affairs, legislative affairs, and/or intergovernmental affairs.

This posting will be open until March 23, 2016.

Please visit the [Detail Opportunities page on DHS Connect](#) for the full detail posting as well as other detail opportunities across DHS.



Treasury Executive Institute - Cornell Leadership Certificate Program Accepting Applications

The [Treasury Executive Institute](#), in partnership with Cornell University, is now accepting applications for its Executive Leadership Certificate Program. This program consists of six, two-week classes authored by Cornell University faculty with live instruction/interaction provided by Cornell experts. The classes which cover OPM’s Executive Core Qualifications include:

- Aligning HR Strategy with Organizational Strategy
- Executive Decision Making
- Managing Strategic Change
- Mobilizing the Coalition for Action
- Tactics and Skills for Negotiating
- The Coaching Process for Engaging and Developing Others

The [application process](#) is open until close of business on March 31, 2016. [Applications](#) should be emailed to LEAD@treasury.gov. Applicants selected will be notified in April.



NPPD Jobs

Employees interested in current NPPD job opportunities and other career-related information and resources should visit the [NPPD Career Center](#) or usajobs.gov. Below are the latest NPPD job listings.

[IT Specialist \(INFOSEC\)](#)

Salary:	\$83,468.00 - \$139,523.00 / Per Year
Series & Grade:	GS-2210-13/14
Location(s):	Multiple Locations (2)
Open Period:	Dec. 18, 2015 – Apr. 18, 2016
Announcement Number:	FS-1553503-CH16
Department:	Department Of Homeland Security
Agency:	National Protection and Programs Directorate
Position Info:	Full Time - Permanent
Who May Apply:	US Citizens

[Special Security Representative](#)

Salary:	\$92,145.00 - \$119,794.00 / Per Year
Series & Grade:	GS-0080-13/13
Location(s):	Washington, D.C.
Open Period:	Mar.14 – Mar. 23, 2016
Announcement Number:	FS-1596018-MQ16
Department:	Department Of Homeland Security
Agency:	National Protection and Programs Directorate
Position Info:	Full Time - Permanent

Who May Apply: US Citizens and Status Candidates

Workforce Management Specialist

Salary: \$77,490.00 - \$119,794.00 / Per Year
Series & Grade: GS-0301-12/13
Location(s): Arlington, Va.
Open Period: Mar. 9 – Mar. 23, 2016
Announcement Number: FS-1624170-SF16
Department: Department Of Homeland Security
Agency: National Protection and Programs Directorate
Position Info: Full Time - Permanent
Who May Apply: US Citizens

Program and Management Analyst

Salary: \$77,490.00 - \$119,794.00 / Per Year
Series & Grade: GS-0343-12/13
Location(s): Washington, D.C.
Open Period: Mar. 14 – Mar. 23, 2016
Announcement Number: FS-1631769-MD16
Department: Department Of Homeland Security
Agency: National Protection and Programs Directorate
Position Info: Full Time - Permanent
Who May Apply: US Citizens

Operations Research Analyst (Cost Estimator)

Salary: \$92,145.00 - \$141,555.00 / Per Year
Series & Grade: GS-1515-13/14
Location(s): Washington, D.C.
Open Period: Feb. 29 – Mar. 29, 2016
Announcement Number: FS-1606754-LT16
Department: Department Of Homeland Security
Agency: National Protection and Programs Directorate
Position Info: Full Time - Permanent
Who May Apply: US Citizens

IT Specialist (INFOSEC)

Salary: \$53,435.00 - \$100,736.00 / Per Year

Series & Grade:	GS-2210-09/12
Location(s):	Arlington, Va.
Open Period:	Mar. 10 – Mar. 23, 2016
Announcement Number:	FS-1631701-ET16
Department:	Department Of Homeland Security
Agency:	National Protection and Programs Directorate
Position Info:	Full Time – Permanent
Who May Apply:	US Citizens



DHS

Cyber Storm V: Testing the Nation's Ability to Respond to Significant Cyber Incidents

The following blog was posted to dhs.gov on March 16, 2016

Blog By Greg Touhill, Deputy Assistant Secretary for Cybersecurity and Communications, NPPD

Cyber threats to critical infrastructure remain one of our Nation's most serious security and economic sustainability challenges. With over 80 percent of critical infrastructure owned by the private sector, and with millions of cyber-dependent equities owned by individuals or federal, state, local, tribal, and territorial (SLTT) entities and agencies, securing cyberspace must be achieved collaboratively. Exercises are critical to testing this coordination, and more importantly, to building and maintaining strong relationships among the cyber incident response community.

Last week more than 1,100 people from more than 60 organizations across the country and worldwide participated in the nation's most extensive cybersecurity exercise, hosted by the Department of Homeland Security, Cyber Storm V. The exercise included participants from the healthcare and public health, IT, communications and commercial facilities sectors, as well as federal agencies, eight states, and international organizations.

Participants were presented with a scenario that drove them to exercise their training, policies, processes, and procedures for identifying and responding to a multi-sector cyber attack targeting critical infrastructure. The Cyber Storm V scenario created an environment where no one organization was in a position where they themselves could stop or mitigate the impacts of the attack. The scope of the scenario thus promoted the exercising of cooperation and information sharing across the United States government, states, the private sector, and international partners.

The DHS National Cybersecurity and Communications Integration Center (NCCIC) served as the focal point for federal response and coordination during the exercise. NCCIC is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. NCCIC also is designated as the federal interface for private sector information sharing, cross-sector coordination and incident response

The Cyber Storm V after action process began with a discussion of initial, high-level findings. An after action

conference will help validate these findings and inform the development of an after action report.

For more information about the Cyber Storm exercise series, and to view the final reports from Cyber Storms I-IV, visit <https://www.dhs.gov/cyber-storm>.



Avoiding Online Fraud Takes More than Luck

From the Stop. Think. Connect.™ Campaign

Online fraud, and specifically “phishing,” is a growing problem for Americans and American businesses. Every day, over 80,000 people fall victim to phishing attacks. Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cyber criminals use this stolen information to steal your identity, money, and personal information. Preventing yourself and your company from phishing attacks takes more than just luck. By having an understanding of a few security basics and ongoing vigilance, you can be aware of and defend yourself against these attacks.

Phishing occurs when criminals use a seemingly legitimate email to trick users into providing their sensitive personal information such as social security numbers, passwords, or credit card numbers. When users respond with the information, attackers use it to access their accounts. Cyber criminals may also attempt to lure users to click on a link or open an attachment that infects their computer with viruses or malware, creating vulnerability to attacks. Once the malware is installed, phishers can access your information to hack into your private accounts.

[OnGuardOnline.gov](https://www.onguardonline.gov), a partner of the Stop.Think.Connect.™ Campaign, has provided the following examples of what verbiage a phishing email may include so you can be better prepared to identify these scam emails:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must send us your account information within 7 days to receive your refund."

Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via email or text. Also look for poorly-worded emails. If an email “sounds” off when you read it, this could be a sign that it was not written by a legitimate source. You can also call the company’s customer service number and verify that this email is truly from them.

The [Stop.Think.Connect. Campaign](https://www.stopthinkconnect.com) encourages all Americans to take the following steps to protect yourself against online scams:

- **When in doubt, throw it out:** Links in email and online posts are often the way cyber criminals compromise your computer. If it looks suspicious – even if you know the source – it’s best to delete or, if appropriate, mark it as ‘junk email.’
- **Be wary of email attachments:** Be cautious of email attachments from unknown sources. Many viruses can fake sender addresses, so even if a message looks like it’s from someone you know, think twice about opening any attachments – as they may be infected with malware.
- **Install and update anti-virus software:** Make sure all of your computers are equipped with antivirus software, firewalls, email filters, and anti-spyware. Last year, 99.9% of data breaches reported by Verizon

were a result of hackers exploiting bugs on user's devices that had fixable patches, but just hadn't been installed yet.

- **Think before you act:** Be wary of communications that implore you to act immediately, offers something that sounds too good to be true, or asks for personal information.

How to Report Phishing Attempts

To report suspected phishing attempts, visit the Anti-Phishing Working Group (APWG) at www.apwg.org. The United States Computer Emergency Readiness Team (US-CERT) collects phishing email messages and website locations to help people avoid becoming victims of phishing scams. To report suspected phishing attempts, visit www.us-cert.gov/report-phishing.

Visit the National Cyber Security Alliance's [Spam and Phishing](#) page for more information on how to protect yourself against these attacks.



TIP OF THE WEEK

Enjoy the Cherry Blossoms

Spots of pink and white are finally decorating the Tidal Basin and soon it'll be all pink as the cherry blossoms will likely reach peak bloom later this week. Nothing signifies the arrival of spring in the Nation's Capital quite like the blooming of the cherry blossoms, an event that has spawned a three-week festival celebrating the occasion. More than 1.5 million visitors descend upon Washington, D.C. each year.



The National Cherry Blossom Festival is a spring celebration in Washington, D.C. commemorating the March 27, 1912 gift of Japanese cherry trees from Mayor Yukio Ozaki of Tokyo City to the city of Washington. Mayor Ozaki donated the trees in an effort to enhance the growing friendship between the United States and Japan and also celebrate the continued close relationship between the two nations. The cherry blossom blooming period is a relatively brief window—a week or two, really—when they go from just buds to beautiful flowers to falling off and being replaced by green leaves. The cherry blossoms are racing through their development thanks to the unseasonably warm winter we experienced. NPS is now predicting that the trees will be at peak bloom March 18-23.

Here are the tips for making your cherry blossom visit a pleasant and productive one:

- Don't drive if possible, walk or take the metro
- Visit on a weekday if you have the flexibility
- Have your camera ready
- Visit during peak season (March 18-23 this year)
- Popular places to see the blossoms include the Jefferson memorial, the Martin Luther King Jr. Memorial and the Franklin D Roosevelt Memorial.
- "Off the radar" cherry blossoms can be found US National Arboretum

For more information, please visit: <http://www.nps.gov/subjects/cherryblossom/index.htm>



NPPD VISION is a weekly e-newsletter featuring stories about employees and resources for employees including updates on training, professional development and other NPPD and DHS-related news. Please send any feedback and input to NPPDVISION@hq.dhs.gov.

Content for NPPD Vision must be submitted via email to NPPDVision@hq.dhs.gov by close of business Tuesday for inclusion in the next week's issue. Content should follow all [submission guidelines](#).

-
NPPD VISION is produced and distributed by NPPD's Office of Public Affairs:

Senior Editor: (b) (6)

Managing Editor: (b) (6)

Editor: (b) (6)