Wireless Access Monitoring - OPM checks for unauthorized wireless access to the Local and Wide Area Network (LAN/WAN) by monitoring all Virtual Private Network (VPN) traffic from remote devices. Suspicious activities from VPN connections are investigated to validate risks and perform remedial actions as necessary.

Two-Factor Authentication - OPM authorizes wireless access via two-factor authentication to OPM's VPN. All external OPM wireless access is technically forced to authenticate to OPM's VPN prior to establishing connectivity to the network.

Access Control Enforcement - Enforcement of OPM's wireless access controls is technically accomplished with FIPS 140-2 approved VPN authentication. Enforcement is also implemented through continuous monitoring and ongoing assessments of existing planned controls.

RIGHT TO PRIVACY

Activity on Government computers is monitored for security reasons. When you log on to a government system, you give your consent to this monitoring; therefore, the right to privacy does not apply to your computer use. Also, keep in mind that the following activities or Websites are prohibited on Government computers:

- **Adult Content**
- **Gambling**
- **Private Business Activities**
- **Unauthorized Configuration Changes**
- **Online Auctioning**

.GOV EMAIL ACCOUNT

Your OPM email address is only for **OFFICIAL** government activities and not used for personal use on any website. This will reduce the potential for compromise. If you have used your .gov email address, change your account information to an alternate/personal email account.

Lesson 2

PRIVACY

What You Will Learn

After completing this training module, you will:

- Understand what Personally Identifiable Information (PII) is
- Understand your responsibility to safely handle PII
- Know how to recognize and respond to a breach of PII
- Know your obligations under the Privacy Act and the e-Government Act

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PERSONALLY IDENTIFIABLE INFORMATION (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Common examples of PII include:

- Name (name by itself is PII)
- Social Security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Financial records, including bank account or other financial account numbers (Credit card information)
- Address (both physical and email)
- Retirement account number
- Health information
- Business contact information (Phone number)
- Driver’s license number
- Passport number
- Race and Ethnicity
- Sex
- Gender
- Disability
- Biometric Identifiers

Because there are many types of information that can be used to distinguish or trace an individual's identity, this definition is necessarily broad – and not limited to the above list.

Information that on its face does not appear to be PII can become PII if it is linked, or linkable, to another piece of information about a particular individual. For example, yellow shirt or brown hair when used to distinguish one person from another are PII, whereas standing alone and not linked or linkable to an individual they are not.

SENSITIVE PII

The loss or compromise of some PII can cause harm to an individual – to include financial harm, embarrassment, or unfairness. The sensitivity of PII must be evaluated in context to determine the risk of harm to an individual in the event of a loss or compromise. For example, a list of names in a public directory may not be sensitive, but a list of names of individuals who received poor performance reviews is.
Certain information standing alone is sensitive and creates risk to an individual. For example, personal financial account numbers, drivers' license or state ID numbers, and biometric identifiers, alone, are sensitive PII. Social Security numbers (SSNs) are also a common example of sensitive PII. Other PII is sensitive in combination: For example, a date of birth combined with an individual's name is sensitive PII, whereas standing alone and not linked or linkable to another identifying data element it is not.

HANDLING PII

Protecting PII is everyone's responsibility. Be aware of what PII you have in your possession and the PII that resides in any electronic system you access. Be vigilant when handling PII so that it is not lost or compromised. To that end:

- Limit your access to only the PII that you have a need to know and do not disclose or provide access to others unless they also have a need to know for a legitimate business purpose.
- Do not leave documents containing PII visible or unattended on your desk. At the end of the day, either secure them in a locked office or in a locked drawer. Lock your computer and remove your PIV card when leaving your laptop, even for a brief time.

HANDLING PII - Email

- When sending PII over email or responding to an email containing PII, double check email addresses to make sure you have selected the correct recipients and double-check your attachment to make sure you have selected the correct document. Ask yourself: is there any PII in the message? Where is the PII located in the message? Where are you sending the email? Never include a SSN or PII as a reference number on tracking forms, return receipts or envelopes or packages.

- When emailing PII, be aware that the autofill function may populate the wrong recipient, and you should take care to check that you are sending the email only to those who have a need to know the information for a legitimate business need. If you are sending to multiple people or a distribution list, make sure what you are sending is appropriate for every recipient.

- Only send sensitive PII via email using "Send Secure" or other means approved by the Chief Information Security Officer. Sensitive email sent internally within OPM does not require additional encryption however, users should share files via OCIO approved technologies such as OneDrive, Teams, or SharePoint rather than including sensitive attachments. In either case, consider the business need and check your message carefully before sending PII to either external or internal parties.

HANDLING PII - Printers and Fax Machines

- Do not leave documents containing PII unattended at a printer. If you are printing PII to a shared printer, verify the location of the printer prior to sending the document to print and immediately retrieve the printed material.

- Likewise, when you send PII via Fax machine, doublecheck fax numbers before dialing, and before transmitting and call the recipient BEFORE and AFTER the transmission for verification it was received by the right person.

HANDLING PII - Oral Communication

- Do not discuss PII in public places, such as restaurants, elevators, hallways, bathroom, or outside OPM, where others without a need to know may hear the discussion.

HANDLING PII - Mail

- Dispose of documents containing PII appropriately, such as by shredding or placing in a locked bin or burn bag. Do not place them in a trash can or general recycling bin.

- When mailing PII, make sure that only information intended for the recipient to whom the mail is addressed is included in the envelope. Do not mark the envelope in any way that would call attention to the fact the sensitive information is enclosed. If possible, all such mailings should be sent in a manner that can be tracked, such as return receipt requested, so that you are certain it has reached its intended recipient.

HANDLING PII - Teleworking

There are additional considerations in place for protecting PII in telework locations.

Program offices may have their own respective policies in place for transporting PII. Generally, moving PII from your OPM location to home and back requires supervisory approval. You should provide your supervisor with a list of all printed documents to be moved to ensure accountability of documents. PII should be physically secured while in transit. Documents should not be left in plain sight or unattended in a private vehicle or other modes of transportation.

While teleworking, either in a maximum telework or routine telework situation, please be extra careful of leaving PII exposed that others in your household may inadvertently see and make sure the PII materials are disposed of properly. Only use OPM-approved portable electronic devices and password-protect all documents containing PII. You should secure all notes, documents, and portable media devices when not in use. Make sure that you keep your work files separate from personal files. Do not forward work emails to your personal or web-based email accounts. Do not take personnel-related data home without permission of your supervisor. Do not leave personnel-related data unattended at home.

Only government-furnished printers (designated by OPM's OCIO) may be used at an alternative site. Do not print OPM documents on a personal home printer. Government-furnished printers may be used only by OPM employees, and not by family members. If employees have been approved to print documents at home, they must maintain a controlled environment for printed documents, such as a locking cabinet or locked office. Other individuals, including family members, should not have access to printed documents.

Employees should dispose of all printed materials (including drafts, and PII) appropriately using a cross-cutting shredder. Program offices may purchase shredders approved for purchase by CIO. If your office does not purchase a shredder for an alternative site, you are still responsible for shredding documents privately, or securely transporting materials to OPM and use the office shredder or place in OPM's protected bins.

Make sure that any shared network folder where you store PII is accessible only to those who have a need to know the information for a legitimate business purpose.

As a reminder, regardless of where printed records are kept at the office or in a telework environment, they are part of the OPM records system and are subject to the requirements of the OPM records management program.

Vulnerable Areas Where PII Can Be Compromised - Trash

- Dispose of unwanted documents or disks containing sensitive data appropriately. Use the burn bags and locked trash bins for sensitive material.
- Use caution when discarding information in your waste bin. Once trash leaves the office, we lose control over it, and it can become vulnerable. Think about what someone could find out about you or your work if they examined documents in your waste bin!
- Sensitive documents must be shredded or placed in an area where the paper will be picked up and shredded later.

Vulnerable Areas Where PII Can Be Compromised - Fax Machines and Printers

- Double check fax numbers before dialing, and before transmitting, to ensure you have the correct number.
- Call the recipient BEFORE and AFTER the transmission for verification it was received by the right person.

- Verify your printer location PRIOR to sending a document to the printer.
- Promptly pick up ALL copies of the documents.
- Dispose of sensitive documents appropriately, e.g., shred them.
- Use a special trash receptacle for sensitive papers or a paper shredder.

BREACHES OF PII

Sometimes, regardless of how careful you are in handling PII, it may be lost or compromised. This is a "breach," defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. OMB Memorandum M-17-12, Preparing for and Responding to Breach of Personally Identifiable Information.

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII electronically, by, for example, a network intrusion, a targeted attack exploiting website vulnerabilities, or an attack executed through an email message or attachment.

A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, an oral disclosure of PII to a person who is not authorized to receive that information, or inadvertently sending an email containing PII to a recipient who does not have a business need to receive the information.

COMMON BREACH SCENARIOS

The following are some common breach scenarios:

- A laptop or portable storage device storing PII is lost or stolen.
- An email containing PII is inadvertently sent to the wrong party.
- A box of documents containing PII is lost or stolen during shipping.
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits.

- A user with authorized access to PII uses it for personal gain or disseminates it to embarrass an individual.
- An IT system that maintains PII is accessed by a malicious actor.
- Mail enclosing PII sent out from OPM is either not sealed or PII information is visible when the letter is enclosed in a window envelope.
- PII that should not be widely disseminated is posted inadvertently on a public website.

REPORTING A BREACH

IMMEDIATELY report ANY breach by emailing CyberSolutions@opm.gov or by calling 844.377.6109. Also, notify your supervisor. Report all losses or potential losses of PII, regardless of whether you think it is sensitive or not.

Reporting a breach is necessary so that appropriate steps can be taken to mitigate the breach and minimize the risk to the individuals whose PII may have been compromised. All breach reports submitted to CyberSolutions are reviewed by Office of Executive Secretariat and Privacy and Information Management staff.

Social Security Number Justification

Authorities

- OMB Circular No. A-130, Managing Information as a Strategic Resource

Policy

- All OPM personnel shall reduce or eliminate the use of SSNs wherever possible
- Use of the SSN includes the SSN in any form, including, but not limited to, truncated, masked, partially masked, encrypted, or disguised SSNs
- SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria
- SSNs shall be used in approved forms and systems when they meet one or more of the acceptable use criteria
- Specific reviews of forms and systems shall be conducted to reduce SSN use

FAIR INFORMATION PRACTICE PRINCIPLES (FIPPs)

The Fair Information Practice Principles (FIPPs) are a collection of widely accepted principles that provide a consistent framework for analyzing, evaluating, and developing policy concerning our collection, maintenance, use, and dissemination of personally identifiable information (PII) and the effect on individual privacy. As articulated most recently in the Office of Management and Budget Circular A-130, the FIPPs are:

Access and Amendment: provide individuals with appropriate access to and ability to correct their information.

Accountability: be accountable for and document compliance with applicable privacy requirements.

Authority: collect, maintain, and use PII only if you have the authority to do so.

Minimization: collect, maintain, and use only PII that is directly relevant and necessary to accomplish a legally authorized purpose.

Quality and Integrity: collect, maintain, and use PII that is as accurate, relevant, timely, and complete as is reasonably necessary to ensure fairness to the individual.

Individual Participation: involve the individual in the process of using their PII and seek consent where practicable.

Purpose Specification and Use: provide notice of the specific purpose for which PII is collected and only use, maintain, or disclose it for that purpose.

Security: establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use and destruction.

Transparency: be transparent and provide notice about information policies and practices concerning PII.

To learn more about the FIPPs, please watch this Federal Privacy Council video.

THE PRIVACY ACT

The Privacy Act is the cornerstone of federal privacy law and provides rights and protections for individuals whose information the Executive Branch requires to carry out its mission of serving the American people. The Act balances the government's need to maintain information about individuals with the rights of those individuals to be protected from unwarranted invasions of their privacy. It does this by:

- Restricting the disclosure of individuals' information.
- Providing access and amendment rights to individuals whose information has been collected; and
- Establishing a set of fair information practice principles regarding the collection, maintenance, use, and dissemination of individuals' information.

More specifically, the Privacy Act applies to records about U.S. citizens and lawful permanent residents contained in an agency "system of records." A "system of records" is a group of records from which information is retrieved by a name or other identifier. For every system of records, an agency must publish a system of records notice, or SORN, in the Federal Register. A list of OPM's SORNS can be found at https://www.opm.gov/privacy.

To learn more about the Privacy Act of 1974, please watch this Federal Privacy Council video.

THE E-GOVERNMENT ACT and PRIVACY IMPACT ASSESSMENTS

The E-Government Act requires you to conduct a Privacy Impact Assessment (PIA) whenever you develop, procure, or use information technology to create, collect, store, process, maintain, disseminate, or dispose of personally identifiable information (PII). The assessments are documented and presented to the public on OPM's website, and these documents provide transparency to the public about OPM's collection, use, and dissemination of PII.

A PIA explains what information is being collected, how OPM intends to use that information, who it will be shared with, how it is secured, and whether individuals can approve or decline the use of their information. The PIA employs the FIPPs to identify and evaluate privacy risk by, for example, examining whether only the minimum information needed to achieve the intended purpose is collected and whether mechanisms are in place to reasonably ensure accuracy.

OPM's PIAs are available at https://www.opm.gov/privacy.

To learn more about Privacy Impact Assessments, please watch this Federal Privacy Council video.

Lesson 3
THREATS

WHAT IS A CYBERSECURITY THREAT?

NIST defines a Threat as, *"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."*

THREAT SOURCES

The following is a listing of potential Threat Sources:

HUMAN - ADVERSARIAL

Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).

- **INDIVIDUAL** (Outsider, Insider, Trusted Insider, Privileged Insider)
- **GROUP** (Ad Hoc, Established)
- **ORGANIZATION** (Competitor, Supplier, Partner, Customer)
- **NATION STATE** (Foreign Nation)

HUMAN - ACCIDENTAL

Erroneous actions taken by individuals in the course of executing their everyday responsibilities.

- **USER** (General users of an information system)

- **PRIVILEGED USER/ADMINISTRATOR** (Users with advanced system permissions)

STRUCTURAL

Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.

- **IT EQUIPMENT** (Storage, Processing, Communications, Display, Sensor, Controller)
- **ENVIRONMENTAL CONTROLS** (Temperature/Humidity, Power Supply)
- **SOFTWARE** (Operating System, Networking, General-Purpose Application, Mission-Specific Application)

ENVIRONMENTAL

Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.

- **NATURAL OR MAN-MADE DISASTER** (Fire, Flood, Tornado, Hurricane, Earthquake, Bombing, Overrun)
- **UNUSUAL NATURAL EVENT** (Sunspots, Meteor Shower)
- **INFRASTRUCTURE FAILURE/OUTAGE** (Telecommunications, Power Grid)

THREAT ATTACK METHODS

There are many attack methods utilized by Threat Actors. Here are the most common encountered.

SOCIAL ENGINEERING

Social Engineering is an attack vector used to gain access to networks, systems, or physical locations, or for financial gain by using human psychology, rather than using technical hacking methods. It relies on social interaction to manipulate people into circumventing security best practices and protocols.

Social engineering is the new preferred tactic among the hacker community. It is easier to exploit users' flaws than to discover a vulnerability in networks or systems.

Social Engineering is based on taking advantage of the following:

Heightened Human Emotions - Emotional manipulation gives attackers the upper hand in an interaction. You are far more likely to take irrational or risky actions when in an enhanced emotional state. The following emotions are all used in equal measure to convince you.

These emotions include: Fear, Excitement, Curiosity, Anger, Guilt, and Sadness.

Urgency - Time-sensitive opportunities or requests are another reliable tool in an attacker's arsenal. You may be motivated to compromise yourself under the guise of a serious problem that needs immediate attention. Alternatively, you may be exposed to a prize or reward that may disappear if you do not act quickly. Either approach overrides your critical thinking ability.

Trust - Believability is invaluable and essential to a social engineering attack. Since the attacker is ultimately lying to you, confidence plays an important role here. They've done enough research on you to craft a narrative that's easy to believe and unlikely to rouse suspicion.

MALICIOUS CODE

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.

HACKING

Hacking is the process of gaining unauthorized access to a computer network or an electronic device. Individuals breach into a system either to cause harm or to highlight vulnerabilities in existing security measures.

There are some others whose motives remain ambiguous or even double-sided. Hackers are of six main types:

WHITE HAT HACKER - White hat hackers are the ethical hackers who use their skills to discover loopholes in existing cybersecurity measures to help fix them.

BLACK HAT HACKER - Black hat hackers are malicious individuals in cyberspace who try and break into systems & networks to steal confidential information. In addition to stealing, a black hat hacker may also delete or modify certain crucial files to cause disruption and inflict losses.

GRAY HAT HACKERS - Grey hat hackers use methods that are similar to those of white and black hat hackers. However, they do not have any malicious intentions. A gray hat hacker may breach into a company's private servers, but instead of stealing information, will notify management about the vulnerability.

RED HAT HACKER - Red hat hackers are similar to policing agents on the internet. They actively search for black hat hackers and shut them down. Whenever they find one, they don't report the hacker to the authorities, but take matters into their own hands. A red hat hacker will hack the would-be attackers' computer and halt their malicious activities.

BLUE HAT HACKER - A blue hat hacker can be malicious but usually, that anger is channeled at one person or company. They seek revenge for some type of wrong. Blue hats are typically new to hacking and may start out as Script Kiddies. An event or incident may turn them from being nonchalant about hacking to being focused on exacting some kind of hacking catastrophe for their target.

GREEN HAT HACKER - Green hat hackers are newbies, and they are working to improve their skills every day so they can become better. The green hat has something to prove and often gets chided by the hacking community if they ask basic questions. Yet, their desire to learn keeps them asking. They may idolize well-known black hats and are desperate to elevate themselves to the real world of hacking.

HACKTIVISTS - Hacktivists break into government or corporate systems out of protest. They use their skills to promote a political or social agenda. Targets are usually government agencies or big corporations.

SCRIPT KIDDIES - Script kiddies are hackers who are new to hacking and don't have much knowledge or skills to perform hacks. Instead, they use tools and scripts developed by more experienced hackers.

DENIAL OF SERVICE

A Denial-of-Service (DoS) is any type of attack where the attackers attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid

return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

DISTRIBUTED DENIAL OF SERVICE

A Distributed Denial-of-Service (DDos) is a consorted event where multiple attackers or entities coordinate a DoS attack on a specific resource.

Clickjacking

Clickjacking - Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both. (OWASP.org).

THREAT - SOCIAL ENGINEERING

This attack vector relies on social interaction to manipulate people into circumventing security best practices and protocols.

PHISHING

Phishing is the most common type of social engineering attack that occurs today. Most phishing scams endeavor to accomplish three things:

- Obtain personal information such as names, addresses and Social Security Numbers.
- Use shortened or misleading links that redirect users to suspicious websites that host phishing landing pages.
- Incorporate threats, fear, and a sense of urgency in an attempt to manipulate the user into responding quickly.

DECEPTIVE PHISHING

Deceptive phishing is by far the most common type of phishing scam. In this ploy, fraudsters impersonate a legitimate company in an attempt to steal people's personal data

or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.

SPEAR PHISHING

Not all phishing scams embrace "spray and pray" techniques. Some ruses rely more on a personal touch. They do so because they wouldn't be successful otherwise.

In this type of ploy, fraudsters customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender. Yet the goal is the same as deceptive phishing.

Given the amount of information needed to craft a convincing attack attempt, it's no surprise that spear-phishing is commonplace on social media sites like LinkedIn where attackers can use multiple data sources to craft a targeted attack email.

WHALING

Spear phishers can target anyone in an organization, even executives. That's the logic behind a "whaling" attack. In these scams, fraudsters try to harpoon an exec and steal their login details.

VISHING

This type of phishing attack dispenses with sending out an email and instead goes for placing a phone call. An attacker can perpetrate a vishing campaign by setting up a Voice over Internet Protocol (VoIP) server to mimic various entities in order to steal sensitive data and/or funds.

SMISHING

This method leverages malicious text messages to phones to trick users into clicking on a malicious link or handing over personal information.

PHARMING

As users become wiser to traditional phishing scams, some fraudsters are abandoning the idea of "baiting" their victims entirely. Instead, they are resorting to pharming. This method of phishing leverages cache poisoning against the domain name system (DNS), a naming system which the Internet uses to convert alphabetical website names, such as "www.microsoft.com," to numerical IP addresses so that it can locate and thereby direct visitors to computer services and devices.

PRETEXTING

Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they use to try and steal their victims' personal information. In these types of attacks, the scammer usually says they need certain bits of information from their target to confirm their identity. In actuality, they steal that data and use it to commit identity theft or stage secondary attacks.

More advanced attacks sometimes try to trick their targets into doing something that abuses an organization's digital and/or physical weaknesses. For example, an attacker might impersonate an external IT services auditor so that they can talk a target company's physical security team into letting them into the building.

Whereas phishing attacks mainly use fear and urgency to their advantage, pretexting attacks rely on building a false sense of trust with the victim. This requires the attacker to build a credible story that leaves little room for doubt on the part of their target.

Pretexting can and does take on various forms. Even so, many threat actors who embrace this attack type decide to masquerade as HR personnel or employees in the finance department.

BAITING

Baiting is in many ways similar to phishing attacks. However, what distinguishes them from other types of social engineering is the promise of an item or good that malicious actors use to entice victims. Baiters may leverage the offer of free music or movie downloads, for example, to trick users into handing over their login credentials.

Baiting attacks are not restricted to online schemes. Attackers can also focus on exploiting human curiosity via the use of physical media.

QUID PRO QUO

Similar to baiting, quid pro quo attacks promise a benefit in exchange for information. This benefit usually assumes the form of a service, whereas baiting usually takes the form of a good.

Popular baiting comes from actors pretending to be from employees of the Social Security Administration (SSA) or Internal Revenue Service (IRS).

CLICKJACKING

Clickjacking, also known as a “UI redress attack”, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is “hijacking” clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both. (OWASP.org).

PHYSICAL

Some Social Engineering relies on the physical presence of the threat actor to perpetrate.

TAILGATING

In these types of attacks, someone without the proper authentication follows an authenticated employee into a restricted area. The attacker might impersonate a delivery driver and wait outside a building to get things started. When an employee gains security’s approval and opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building.

Tailgating, also known as "piggy backing", does not work in all corporate settings such as large companies whose entrances require the use of a keycard. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to get past the front desk.

SHOULDER SURFING

In this type of attack someone can sneak up next to or behind a person to view the information on the computer screen of a user without their knowledge.

EAVESDROPPING

In this type of attack someone lurking nearby can listen in on person-to-person conversation (as well as phone conversation) when individuals are discussing sensitive information that could be used in other Social Engineering endeavors.

BORROWING

In this type of attack someone may ask to use your phone or computer to access a site or lookup their email because theirs is not working, or they forgot it at home. This will give them access to your personal resources and access privileges.

THREAT - MALICIOUS CODE 1

This attack vector relies on installation of computer code (software or firmware) that circumvent implemented security programs and protocols.

VIRUSES

A virus is a malicious program that modifies other host files or boot areas to replicate. In most cases the host object is modified to include a complete copy of the malicious code program. The subsequent running of the infected host file or boot area then infects other objects.

WORMS

A worm is a sophisticated piece of replicating code that uses its own program coding to spread, with minimal user intervention. Worms typically use widely available applications (e.g., email, chat channels) to spread. A worm might attach itself to a piece of outgoing email or use a file transfer command between trusted systems. Worms take advantage of holes in software and exploit systems. Unlike viruses, worms rarely host themselves within a legitimate file or boot area.

TROJAN HORSES

A Trojan, or Trojan horse, is a nonreplicating program masquerading as one type of program with its real intent hidden from the user. For example, a user downloads and runs a new, free version of his favorite multiplayer game from a web site. The game promises thrills and excitement. But its true intent is to install a Trojan routine that allows malicious hackers to take control of the user's machine. A Trojan does not modify and infect other files.

THREAT - MALICIOUS CODE 2

This attack vector relies on installation of computer code (software or firmware) that circumvent implemented security programs and protocols.

KEYLOGGER

A specific type of spyware is known as a keylogger (or a “keystroke logger” for you more specific readers). A keylogger is a type of hardware or software that records everything you type without needing access to what’s on your monitor. That’s because it records all of your keyboard activities — basically, every keystroke you type on your keyboard. The benefit of this to hackers is that it allows them to monitor your activities and capture sensitive information such as your account credentials and passwords.

ROOTKITS

A rootkit is a remote access tool (RAT) or application that provides remote admin access to devices. This isn’t bad in and of itself. But, as you can imagine, this means that they can cause a lot of damage if they’re put to work by someone with devious intentions.

BOTS AND BOTNETS

A botnet is a network of compromised computers, servers, and Internet of Things (IoT) devices (infected devices that are also sometimes called bots or zombies). The devices are infected with a malware and form a massive weapon that cybercriminals can use to launch massive, distributed denial of service (DDoS) attacks against individuals, governments, and organizations. These attacks inundate the target with traffic requests or packets to disrupt the server or network, or to take it offline completely.

THREAT - MALICIOUS CODE 3

This attack vector relies on installation of computer code (software or firmware) that circumvent implemented security programs and protocols.

ADWARE

Adware is not in itself malware but is an embedded portion of software that periodically pushes ads inside the application running or as popups. In some instances, Adware can sometimes assist in the delivery of other malware, which may often include spyware. Adware can just as easily be harmless and respectful, whereas others might be invasive and irritating.

SCAREWARE

Scareware is a malware tactic that manipulates users into believing they need to download or buy malicious, sometimes useless, software. Most often initiated using a pop-up ad, scareware uses social engineering to take advantage of a user's fear, coaxing them into installing fake anti-virus software.

RANSOMWARE

Ransomware is a type of malware that encrypts a target's data until some demand is satisfied — typically, the payment of a ransom. (Hence the clever malware name.)

THREAT - INSIDER

An insider is anyone given approved access to an agency's system and information (data) resources and through an action/activity initiated by them and causes harm to the agency's system and/or information resources. Their approved access can be current or expired. Insiders can include current or former employees, contractors, or business partners.

MALICIOUS INSIDER

A Malicious Insider is one who maliciously and intentionally abuses legitimate credentials, typically to steal information for financial or personal incentives. Malicious Insiders have an advantage over other attackers because they are familiar with the security policies and procedures of an organization, as well as its vulnerabilities.

Other forms of the Malicious Insider are:

- **Professional Insider** - An Insider with the knowledge and intent to circumvent security policies and procedures to exploit the agency's system and information resources. This includes the printing and copying of sensitive information (e.g. PII, and Financial Information).
- **Insider Agent** - A person working with another Threat Source (Insider or Hacker) to provide access to resources or information to exploit weaknesses.

NEGLIGENT INSIDER

A Negligent Insider is one who intentionally or unintentionally through their inaction/inactivity causes the exploit of the agency's system and information resources or abuses legitimate credentials, typically to steal information for financial or personal incentives. Malicious Insiders have an advantage over other attackers because they are familiar with the security policies and procedures of an organization, as well as its vulnerabilities.

ACCIDENTAL INSIDER

An Accidental Insider is one who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to an organization’s information or information systems. The Accidental Insider usually performs an action or activity contrary to organizational security guidance or security best practices.

THREAT - INSIDER - EXAMPLE

Difference between a Malicious and Accidental Insider Threat

MALICIOUS

The disgruntled employee was upset over not being promoted to a new position and wanted to get even with management.

The User has access to system resources and bad intent to cause harm to the agency's system and information resources.

ACCIDENTAL

A new unsupervised employee deletes the wrong customer account.

The User has access to system resources but does not have bad intent to cause harm to the agency's system and information resources.

CYBER ALERT RELATED TO WORLD EVENTS

CYBER ALERT RELATED TO WORLD EVENTS

Many world events are on the minds of individuals around the globe. Unfortunately, cyber-attackers are likely to use the public's interest and concern to their advantage. History has shown that cybercriminals monitor current events closely, quickly developing and distributing malicious content, including:

• Phishing emails, text messages, and phone calls

• Fraudulent online ads and social media posts

• Lookalike websites

You might encounter threats in the form of:

• Sensationalized stories that seem to come from legitimate news outlets

• Inflammatory claims and other forms of misinformation

• Fake charity and assistance organizations

Those who engage with fraudulent content could reveal sensitive personal data or expose themselves (and our organization) to malicious software (malware).

You must remain alert to attackers' attempts to manipulate you and trick you into taking a dangerous action. Apply what you've learned in your security awareness training to ensure you're making the best choices. Be sure to report ANY suspicious emails by clicking the "Report Phishing" button in Outlook.

Lesson 4

CYBER-DEFENSE

LINES OF CYBER-DEFENSE

Like a castle defending against a siege, OPM has several layered security defenses to protect its information systems, data, and personnel from threat actors.

DATA LAYER - is where all OPM's information resides. At this layer the data is protected when at rest (stored) and while in transport (being processed by an application or transmitted across the network).

APPLICATION LAYER - is where data is processed and accessed by users. This layer uses protection mechanisms that promote "**Least Privilege**" (the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function) and "**Separation of Duties**" (also known as "Keys to the Kingdom", this refers to the principle that no user should be given enough privileges to misuse the system on their own).

ENDPOINT LAYER - is where applications reside, operate, and connect to networked resources. Hardware devices that reside on the agency's network (.e.g Computers, Phones, Printers, etc.) where applications reside and operate.

NETWORK LAYER - is the hardware and software infrastructure that connects all endpoints together and manages the communications between those devices as well as external through the perimeter.

PERIMETER LAYER - is the hardware and software infrastructure that connects the internal OPM network externally (outside OPM). This layer manages all communications between internal and external information resources.

PHYSICAL LAYER - is the physical infrastructure that protect the agency's information assets to include the building, data center, equipment racks, storage cabinets.

POLICY LAYER - this layer provides the rules for development and implementation of the agency's cyber-defense layers to protect agency information assets.

HUMAN LAYER - OPM Federal and Contractor Employees although not part of the OPM's information technology is the best and "**LAST LINE OF DEFENSE**". When all layers fail and a cyber-attack is attempted or successful it is this defense layer where the attack is identified, acted on, and reported.

RESPONDING TO CYBER-ATTACKS

You won't be able to spot every potential cyber-attack, but when an attack occurs you should be ready to act.

PREPARE

Although most cyber-attacks will be stopped through cybersecurity software and tools (e.g. anti-virus, Virtual Private Networks, disk encryption, spam filtering, etc.) there always will be some cyber-attack that gets past these cybersecurity mechanisms. This is why you are a critical part of the effort to stop a cyber-attack.

At some point in your career as a federal or contractor employee you will encounter some form of a cyber-attack. Most cyber-attacks are successful because an individual failed either to follow the guidance provided or did not properly respond to identify, act, or report the cyber-attack.

Take some time to review the Cyber-Defense Prepare - Do's and Don'ts in this lesson to get a good idea of what you should do and not do.

IDENTIFY

As identified in the INTRODUCTION Lesson, "**OUR FIRST LINE OF DEFENSE IS OUR EMPLOYEES**".

The most critical part of the process is the identification of when a cyber-attack occurs or has already occurred.

Take some time and review the "**IDENTIFY A CYBER-ATTACK**" Section of this lesson

ACT

If you encounter a cyber-attack or suspect that a cyber-attack has already occurred **REMAIN CALM** and stop further activities until you document and report the cyber-attack.

Attempt to document what you encountered (what happened and time) for later investigation.

Once you report the cyber-attack you will be given further actions to take.

If the cyber-attack is a Phishing Attempt and you are using the OPM Microsoft Outlook you can, with the suspected email highlighted or open, click the "**Home**" Tab in the upper Menu, then select the "**Report Phishing**" Button in the menu bar.

REPORT

The final step is to report the cyber-attack. It is critical that any identified cyber-attack is reported immediately so that action can be taken to prevent others from encountering the same threat or reduce the overall impact to the agency and its information resources.

To report a cyber-attack, contact the Security Operations Center (SOC) at the following:

EMAIL: *cybersolutions@opm.gov*

PHONE: **844-377-6109**

Follow the instruction given to you by the SOC.

Once reported to the SOC, then contact your supervisor and inform them of the situation.

PREPARE - CYBER-DEFENSE DO

Whenever you access an OPM information system keep in mind the following general **DO** in relation to use of information systems:

- *Do follow security procedures,*
- *Do report security problems, incidents, and suspicious or unusual behavior,*
- *Do recognize the accountability assigned to your User ID and password,*
- *Do log out or lock your workstation before leaving it unattended,*
- *Do limit personal use of your system, especially email and the Internet,*
- *Do keep your laptop and other personal electronic devices safe while traveling,*
- *Do ensure "need to know" before sharing information,*
- *Do shred sensitive documents before disposal.*

PREPARE - CYBER-DEFENSE DON'T

Whenever you access an OPM information system keep in mind the following general things to **DON'T DO** in relation to use of information systems:

- *Do not use a computer to harm other people,*
- *Do not interfere with other people's computer work,*
- *Do not snoop in other people's files,*
- *Do not use a computer to steal,*
- *Do not use or copy software you have not purchased, or have not been approved by the Agency,*
- *Do not steal other people's intellectual property or violate copyright laws,*
- *Do not use a computer to pose as another person,*
- *Do not use other people's computer resources without approval,*
- *Do not share your user ID and password,*
- *Do not install freeware and shareware that has not been tested and authorized for use by your Agency,*
- *Do not allow yourself to be a victim of social engineering or a scam by giving out information to unauthorized individuals.*

PREPARE - MULTIFACTOR AUTHENTICATION

Multi-factor authentication means the use of two out of the following three forms of authorization:

- Something you know (such as a password)
- Something you have such as a PIV card (You will need to know the PIN number associated with your PIV card)
- Something you are (biometric, such as fingerprint, eye)

PREPARE - MAINTAIN YOUR PIV CREDENTIAL

Like your driver's license or credit cards, you are responsible for protecting and caring for the Personal Identity Verification (PIV) Credential. Protective measures you need to take are:

- Keep your Credential in the government-issued badge holder when not in use. These badge holders are specially designed to protect your Credential. Other

containers and plastics, including your wallet, can damage or cause deterioration of the Credential.
- Do not punch holes, bend, mark, or peel any plastic away from the card.
- Do not scratch the magnetic stripe.
- Avoid storing your Credential in areas of extreme heat (e.g., clothes dryer) or sunlight (e.g., car dashboard) as the card could warp.
- Do not allow your Credential near magnetic fields (e.g., stereo equipment, magnets, other magnetic strip cards).
- Do not allow anyone else to use your PIV Credential under any circumstances.

PREPARE - PASSWORDS AND SECRET QUESTIONS

CREATING STRONG PASSWORDS

In some circumstances you will be asked to use some form of authentication other than using your PIV. This mostly will be a Username and Password combination that will let you gain access to information resources and capabilities. Use the following criteria for the development of a Strong Password:

- At least 8 Characters comprised of at least 1 Uppercase Letter, 1 Lowercase Letter, 1 Number, and 1 Special Character (not a letter or number). Privileged accounts require at least 12 characters.
- Should not contain any portion of the account Username or your name.
- Should not contain any common dictionary words.
- Should not contain simple patterns, such as keyboard "qwerty".
- Should not contain variations of the word "password" (.e.g. "P@ssw0rd!").
- Should not be a password that is being used for another application password.

CREATING STRONG SECRET QUESTIONS

In some circumstance you will be asked to create Secret (Golden) Questions that will be used to restore your Password in the event that a reset is necessary. Use the following criteria to Secret Questions:

- At minimum 3 Secret Questions should be created. More than three Security Questions should be created to allow for the rotation of Secret Questions for resets.
- When used for a Password Reset at least 3 Secret Questions must be successfully answered to allow the reset.

- **Safe** - The answers can't be easily guessed or researched.
- **Stable** - The response will not change - Example: Where did you lose your first tooth? Will always be answered: At Aunt Jane's house.
- **Memorable** - So you won't forget it.
- **Definitive/Simple** - Something that requires a specific answer that has a number of answers (e.g. What month did you graduate, there are only 12 months, and most graduations occur from May or June).

PREPARE - SENSITIVE DATA PROTECTION

Sensitive data is that for which loss, unauthorized modification, or unauthorized disclosure would be detrimental to national security operations and generally includes information that meets one or more of the following criteria:

- **Personal in Nature** - Social security numbers, medical information
- **Proprietary** - Contract proposals
- **Financial** - Procurement data
- **National Security Related** - Nuclear power plant blueprints
- **Critical to Agency Plans and Operations** - Network diagrams, password files
- **Shared Agency Information** - Information entrusted to OPM from other Federal Agencies.

All sensitive data must be password protected and kept in a secure place. Care should be exercised concerning the visibility of your computer screen to "over-the-shoulder" viewing, and the proximity of your work area to windows. Additionally, when leaving your desk, you should log off or lock your workstation, and exercise care about leaving sensitive papers on your desk.

Any mobile media (e.g. USB Flash Drives, CD-R, etc.) must be encrypted utilizing FIPS 140-2 validated encryption. In addition, encrypt any sensitive data before sending it electronically. Sensitive data that must be sent via email must be encrypted by typing the words "Send Secure" within the Subject line of the Outlook email. For further information about sending secure email, contact the OPM Help Desk.

PROTECTION OF IRS TAX INFORMATION

In addition to OPM Data Protection Guidance, U.S. Internal Revenue Service (IRS)Tax Information should be protected in accordance with the IRS Publication 1075, "Tax Information Security Guidelines For Federal, State and Local Agencies."

PREPARE - REGULAR BACKUPS

Regular backups minimize data loss from hard drive crashes, virus infections, and so forth. Consequently, you must ensure your files are backed up. You can ask your Help Desk or system administrator for assistance or if you have questions.
Additionally, here are a few backup tips for keeping your files adequately protected:

- *When editing a file create a copy so that you have a copy of the original.'*
- *Identify important files and documents and save them to a Networked Drive.*
- *When collaborating on a file or document utilize "Track Changes" so that you can revert to the original file/document.*
- *If large collaborations use a networked application like SharePoint.*
- *Any documents or information saved on the network drive will be automatically backed up on the network.*

PREPARE - PERSONNEL SECURITY

Personnel security reduces risks through procedures for position staffing and user administration. This ensures role-based and need-to-know access to the system. Personnel security includes, but is not limited to, the following:

- Background screening of job applicants and employees
- Need-to-know access based on job function
- Continual monitoring of employee system usage
- Separation of job duties

PREPARE - TELEWORK

With increased telework it is important to follow these procedures when working with PII data, using a computer or device external to OPM:

CONNECTIONS

- Work in a private location where information that you will be using is not visible to others
- Only use approved equipment to connect to OPM Information Systems and Information
- Connect to OPM Information Systems and Information through approved connections

INFORMATION RESOURCES

- Encrypt any PII data that is stored locally on the computer or device being used to telework
- Follow OPM policies for deleting PII data stored on a computer or device external to OPM to ensure the data is permanently deleted and not recoverable
- Do NOT print out PII data unless previously authorized and the ability to secure, or lock up, any hard copies and shred as necessary
- Do NOT discuss PII data in an environment where you can be overheard

PREPARE - NETWORK CONNECTIVITY

Part of telework is the connection to OPM Information Systems and Information. Use these methods to make a secure connection:

CONNECTING TO A HOME NETWORK

The Help Desk will ensure that your wireless device is working properly on your laptop when you bring it to the Help Desk for configuration and/or troubleshooting. However, because of the number of wireless network devices and numerous configuration options, the OPM Help Desk cannot set up or trouble-shoot individual home network configurations. OPM employees should take the following steps to make sure their home networks are configured correctly and securely:

- Modern wireless equipment for the home, such as Wi-Fi routers, has the capability to be secured. Each device manufacturer has different ways of implementing these security controls, but they all conform to a common set of standards (such as Wi-Fi Protected Access, or WPA).
- OPM employees who wish to use their home wireless networks to access OPM resources should refer to their equipment documentation to make sure they have taken steps to protect their network. Internet Service Providers may also have support phone numbers that employees can call to get assistance securing their wireless home networks.
- Do not share passwords, keys, PINS or other information about home wireless networks with anyone.
- Change device passwords periodically and do not use default passwords set by equipment manufacturers.
- Do not allow anyone, including family members, to use OPM-issued equipment for any reason.
- When you step away from your computer at home, just like you would at work, make sure to lock the system or log off so that no one can use it without your knowledge or permission.

- During setup of wireless equipment at home, always select the option that requires a heightened level of security and password. Do not configure wireless devices so that anyone can access without permission or a password or passphrase.

CONNECTING TO A THIRD-PARTY NETWORK

There are Wi-Fi networks almost everywhere you go these days. Many of these are managed by retail companies that want to provide the service as a way to attract customers. It is extremely important that you know who is running a wireless network before you connect to it. Here are some steps you should follow to make sure you connect securely:

- Do not connect to a wireless network if you are not sure who is running it. For example, if you are in a coffee shop, you may see several Wi-Fi network names when you use your computer. You should only connect to the network run by that coffee shop; if you are not sure which network is the right one, either do not connect at all or ask an employee.
- When traveling, the hotel where you stay may provide wireless access. Often, in order to use these networks, you must verify that you are a guest of the hotel by providing a key or other information. As with the coffee shop example above, make sure to verify with the hotel the proper network and the right procedures.
- It is your responsibility to practice safe computing. Third party wireless networks may be run by someone trying to get access to your Personal Information or other information on your computer. If you are not sure who is managing a wireless network, do not use it!

PREPARE - ENCRYPT SENSITIVE EMAILS

To meet our analysis requirements, all encrypted files and attachments sent or received by our OPM email systems are blocked and quarantined. Such files include password-protected attachments. Commonly encrypted files include PDFs, WinZip files, and Microsoft Office documents. To manage such files, employees should use the following guidelines:

- When emailing encrypted files to approved external recipients, use OPM's enterprise secure messaging portal. For information about this secure method of file transfer, contact: cybersolutions@opm.gov or the OPM Help Desk Self Help web page on the OPM intranet (THEO).
- When you need to receive an encrypted file from an approved external sender, contact cybersolutions@opm.gov. Cybersecurity will perform validation and risk-assessment tasks in order to facilitate a secure transfer of the file.

If you have questions about the secure messaging portal or transferring encrypted files, please email cybersolutions@opm.gov.

IDENTIFY AN EMAIL CYBER-ATTACK

Most cyber-attacks that you will encounter will come from an unsolicited email. These emails will contain some form of mechanism or method (e.g. Social Engineering) to circumvent implemented cybersecurity mechanisms. Some of these include:

Suspicious Emails: Emails from a known or unknown sender with misspellings or asking for unrelated work information or giving instructions to view or download files that were not asked for or not related to a work activity (e.g. "pictures of my vacation"). Look at the FROM: address; the TO: address (is it directly to you or a large group of people); SUBJECT: line; time of day it was sent; and content to misspellings, hyperlinks, and attachments.

Suspicious Hyperlinks: A link in an email that does not go to the correct site as described by the link or that is directed to an unauthorized/unwanted web site such as an unsolicited link to update your account information.

Suspicious Attachments: Attachments that were not requested especially those coming externally from someone other than a co-worker or someone known to you.

Sent Emails: It is a good idea to periodically check your "Sent Mail" Folder to see if there are emails that you did not send. This is a good sign that your email account or application has been compromised.

IDENTIFY AN INTERNET CYBER-ATTACK

Surfing the internet, even an authorized government website, may lead you to internet sites that can initiate a cyber-attack. Some internet things to look out for:

Pop-Ups: Unwarranted pop-ups are not only a nuisance they can be a sneaky way to get you to click on some ad or some other mechanism to redirect you to a nefarious website.

Redirection: In most circumstances you will be notified that you are leaving a website. During a redirection (e.g. going from opm.gov to irs.gov or to another website) if there is a change in the URL root domain (e.g. opm.gov) this may be a cause for alarm.

Installs: When you are asked to install anything (software, plug-ins, add-ons, widgets, etc.) you should not accept. Any installation of software to include browser add-ons and plug-ins, must be approved and performed by the OPM Help Desk or authorization System Administrator.

Reauthentication: In some circumstances you may be required to re-authenticate your credentials when accessing information resources. When asked to provide access credentials assure that the website is an "official" site, and the URL prefix is "https" (a secure website). An unexpected request to provide credentials may be an attempt to capture your login information.

If the website address is something other than what you expect (e.g. an IP Address instead of a URL Address, a .com instead of a .gov) this may be a redirection to an attackers' web page. Also, in some circumstances websites will ask you to load some kind of "plug-in" or "widget" to view the information, create an account, or allow access to your personal computer resources.

IDENTIFY A PHONE CYBER-ATTACK

Although most attempts will come from email and the internet, some threat sources still use the phone (line or cell) to initiate their Social Engineering cyber-attack. These methods include:

Scams: Most phone cyber-attacks are in the form of scams to get you to perform actions based on an urgent need. For instance, this scam, "A call from a person at the IRS stating you owe them money and if you do not pay them immediately, they will issue a warrant for your arrest". This scam usually includes you giving them bank information or going to Western Union to send money to prevent you from being arrested.

Quid Pro Quo: This cyber-attack like a scam offers you something, a prize or money, however, to get it you must pay a fee for processing or effort to deliver. For instance, this may be a call saying that you have inherited a large sum of money and that in order for them to transfer it to you to send them a processing fee.

Vishing: An attacker can perpetrate a vishing campaign by setting up a Voice over Internet Protocol (VoIP) server to mimic various entities in order to steal sensitive data and/or funds.

Impersonation: A common cyber-attack is someone pretending that they are someone that you would normally trust. This trust is used to solicit information from you that could be used in a cyber-attack. For example, someone calls and says they are from the helpdesk, and they received an alert that you have a computer-virus on your PC. They then ask you to authenticate your information so that they can initiate a repair to remove the virus.

Notifications: These are in the form of an alert that someone has broken into your banking account or is charging to your credit card. The person will then ask you to provide your banking or credit card information to verify your account.

IDENTIFY AN IN PERSON CYBER-ATTACK

Although not the preferred method, some cyber-attacks can occur during a direct interaction with a person (someone known or unknown). These interactions prey upon your courtesy and generosity. A common cyber-attack would be a person with their hand full asking you to hold the door open or open the door to a card-access area, like a data center or building that they do not have access to. These types of attacks include:

Impersonator: Similar to other attacks an individual is pretending that they are someone that you would normally trust. This trust is used to solicit information from you that could be used in a cyber-attack.

Borrower: This individual poses as someone that needs help in accessing some resource. They use excuses (my computer is updating, I left my laptop at home, I keep getting an error accessing the website, etc.) to borrow your information resource (computer, phone, etc.) for a short period of time. This not only gives them access to all the resources that you have access to but also leaves an audit trail based on your ID.

Hapless Victim: This individual acts as they are in dire straits and need your assistance. An example is someone carrying coffee and donuts for the entire office asking the security guard to let them in because their hands are full, and they cannot retrieve their credentials.

IDENTIFY A CYBER-ATTACK, KEY AWARENESS

Not all indicators are related to a direct cyber-attack, some are performed in the background without your knowledge or any initial indicator that the cyber-attack occurred. Some things to be aware of are:

Unusual Activities/Actions: Be aware of some actions or activities that were not initiated by you, such as emails in your "Sent Items" email box that were not sent by you.

Resource Availability: Some resources that were previously accessible are no longer accessible because of a permissions change or change to your credentials. This would also

include additional access to resources that you did not request access to or should not have access to, based on work requirements. Also, if information previously stored has been altered or deleted without your knowledge.

Resource Abnormal Behaviors: Some of the resources you are utilizing are acting/behaving abnormal, like your email is slow/sluggish, routine auto-actions are not being performed, like backups or archiving of data. Another is unaware connections to resources other than your own (wireless, Bluetooth, etc.).

Lesson 5

ACKNOWLEDGEMENT

ACKNOWLEDGEMENT OF OPM's SECURITY POLICY AND RULES OF BEHAVIOR

I understand that, when using the OPM Network, I am personally accountable for my actions and must comply with the Rules of Behavior.

I understand the policy is based on Federal laws, regulations, and OPM directives and policies. As such, I understand there are consequences for non-compliance with OPM's Security Policy and Rules of Behavior. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include suspension of access privileges, reprimand, suspension from work, demotion, dismissal, and/or criminal and civil penalties. For any questions regarding the Information Security and Privacy Policy, please email **CyberSolutions@opm.gov**.

I also understand that OPM's computers, networks, and information systems are not "private", and I should have no expectation of privacy when using OPM's computing resources, which is reiterated in OPM's IT System Security Warning Banner. I understand management has the right to monitor, intercept, read, record, and copy information attributable to my access of these resources.

From: Rowell, Danielle R
To: Greg Hogan; Garcia, Carmen E.
Subject: Re: Welcome to OPM - Instructions Prior to Onboarding
Attachments: image001.png

Hi Greg,

Received. Thank you.

Get Outlook for iOS

From: Greg Hogan [redacted]>
Sent: Monday, January 20, 2025 10:24:11 AM
To: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Rowell, Danielle R <Danielle.Rowell@opm.gov>
Subject: Re: Welcome to OPM - Instructions Prior to Onboarding

I have completed the Cybersecurity and Privacy Awareness Training.

Thanks!
Greg Hogan

On Sat, Jan 18, 2025 at 3:33 PM Garcia, Carmen E. <Carmen.Garcia@opm.gov> wrote:

> Good Afternoon,
>
> It gives us immense pleasure to welcome you to our OPM team! We are excited to have you start on Monday and look forward to the valuable contributions we know you will make.
>
> To ensure a smooth transition, we have a few key items for you to review.
>
> ## Training Requirements:
>
> We have attached the OPM cybersecurity training course document for your review. This will provide you with fundamental knowledge about your responsibilities in safeguarding OPM's information systems and resources. Kindly take a moment to go through it before Monday. Once done, please send a confirmation email to Danielle Rowell, our Acting Chief Information Security Officer, at Danielle.Rowell@opm.gov, acknowledging that you have understood the contents.
>
> ## Directions to OPM:
>
> Given the traffic patterns, driving to the Theodore Roosevelt Building can be challenging. However, if you decide to use your personal vehicle, we've arranged a parking pass for you at the guard house on the 20th Street entrance. We've also attached a local public safety map for your convenience. If you prefer not to drive, simply come to the E St. main entrance, where you will be warmly welcomed and escorted into the building.
>
> ## Essentials to Bring:

Please remember to bring along a valid U.S. Passport and a voided check.

We are excited to welcome you to the OPM family and eagerly await your arrival on Monday. If you have cleared security, you will receive or have received a final job offer letter with instructions to complete new hire paperwork. If you are not able to clear before Monday, we will help you complete the forms on Monday. Should you encounter any difficulties in reaching the building, please feel free to reach out to me via call or email.

Have a wonderful weekend!

Carmen

Carmen E. Garcia

CHIEF HUMAN CAPITAL OFFICER | HUMAN RESOURCES DIRECTOR

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E St. NW | Washington DC 20415
Office: (202) 606-1048

For scheduling, please contact: franque'.alexander@opm.gov

OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From: Rowell, Danielle R
To: Brian Bjelde; Garcia, Carmen E.
Subject: Re: completed cybersecuirty training, Brian Bjelde

Hi Brian,
Received. Thank you.

Get Outlook for iOS

From: Brian Bjelde <[redacted]>
Sent: Sunday, January 19, 2025 9:51:03 AM
To: Rowell, Danielle R <Danielle.Rowell@opm.gov>
Cc: Brian Bjelde <bbjelde@gmail.com>
Subject: completed cybersecuirty training, Brian Bjelde

You don't often get email from [redacted]. Learn why this is important

Hi Danielle- I finished the cybersecurity training that was sent to me and was asked to let you know once completed. Thank you!

Regards,
Brian Bjelde

From: Rowell, Danielle R
To: Gavin Kliger
Cc: Garcia, Carmen E.; Saunders, James L
Subject: Re: OPM Security Course

Hi Gavin,

Received. Thank you.

Get Outlook for iOS

From: Gavin Kliger <[redacted]>
Sent: Saturday, January 18, 2025 6:06 PM
To: Rowell, Danielle R <Danielle.Rowell@opm.gov>
Subject: OPM Security Course

> You don't often get email from [redacted]. Learn why this is important

Hello Danielle,

I have read and understood OPM cybersecurity training.

Thanks,
Gavin

From:	Rowell, Danielle R
To:	Riccardo Biasini
Cc:	Garcia, Carmen E.
Subject:	Re: OPM Cybersecurity training - confirmation of completion

Hi Riccardo,

Received. Thank you.

Get Outlook for iOS

From: Riccardo Biasini [redacted]>
Sent: Sunday, January 19, 2025 2:12:27 PM
To: Rowell, Danielle R <Danielle.Rowell@opm.gov>
Cc: Garcia, Carmen E. <Carmen.Garcia@opm.gov>
Subject: OPM Cybersecurity training - confirmation of completion

Dear Danielle Rowell,
Per request from Carmen Garcia (in CC), this email is to confirm that I have reviewed and understood the document "OPM Cybersecurity And Privacy Awareness Training".

Best regards,
Riccardo Biasini

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject:	BIASINI, Riccardo - CLEARED 01/20/2025
Date:	Monday, January 20, 2025 2:40:00 PM
Attachments:	image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Subject: RE: Documentation for Transition Team - Riccardo Biasini
Date: Monday, January 20, 2025 2:24:00 PM
Attachments: image002.png

Thanks Kim!

Nothing further is needed at this time. You will receive a separate EOD message.

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Monday, January 20, 2025 2:09 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Subject: Fw: Documentation for Transition Team - Riccardo Biasini

From: Riccardo Biasini [redacted]>
Sent: Monday, January 20, 2025 1:38 PM
To: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Subject: Fwd: Documentation for Transition Team - Riccardo Biasini

Hi Kimberly,
See signed docs attached.

Best,
Riccardo Biasini

---------- Forwarded message ---------
From: **Riccardo Biasini** [redacted]>
Date: Thu, Jan 16, 2025 at 11:50 AM
Subject: Documentation for Transition Team - Riccardo Biasini
To: <carmen.garcia@opm.gov>

Dear Carmen Garcia,
This is Riccardo Biasini, appointee for an employment in the Federal Employment.
Attached you can find:

- My CV
- Signed OF 306
- Signed SF 86

Please don't hesitate to reach out to me in case you need anything else.

Best regards,
Riccardo Biasini

From:	Dillaman, Miranda C.
To:	Sylke, Kimberly D.
Cc:	Beckman, Christopher J.; Davis, Melinda M.; Hazlett, Amber L.
Subject:	RE: Converting to Permanent Appointment
Date:	Wednesday, March 19, 2025 7:16:00 AM
Attachments:	image002.png

Thanks Kim!

Riccardo will need a full investigation on the 86. Fingerprints are not needed. I will take care of the eApp, email and cc you.

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Tuesday, March 18, 2025 4:32 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Beckman, Christopher J. <Christopher.Beckman@opm.gov>; Davis, Melinda M. <Melinda.Davis@opm.gov>; Hazlett, Amber L. <Amber.Hazlett@opm.gov>
Subject: Converting to Permanent Appointment

Hi Miranda,

I verified the following appointee will move to permanent position:

- Riccardo Biasini (Expert)

He will be on the same PD, please let me know if you need any additional information.

V/R

Kim

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) 936-3339

Email: kimberly.sylke@opm.gov

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject:	BJELDE, Brian - CLEARED 01/17/2025
Date:	Friday, January 17, 2025 7:25:00 AM
Attachments:	image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Lowe, Dana S.; Nickerson, Tiffany V.
Subject: RE: New Hire Information for Incoming Senior Advisor to the Director
Date: Thursday, January 16, 2025 12:04:00 PM
Attachments: image002.png
image003.png

Hi Kim!

I've been notified that Brian Bjelde has been fingerprinted today. Nothing further is required at this time. You will receive a separate EOD message.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Thursday, January 16, 2025 11:41 AM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Beckman, Christopher J. <Christopher.Beckman@opm.gov>; Davis, Melinda M. <Melinda.Davis@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>
Subject: New Hire Information for Incoming Senior Advisor to the Director

Good Morning Miranda,

Requesting temporary clearance (less than 180 days) for Brian Bjelde, incoming Senior Advisor to the Director. Attached are the required documents for your review.

Please let me know if you need any additional information.

V/R

Kim

Kim Sylke (pronouns: she/her)

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) 936-3339

Email: kimberly.sylke@opm.gov

OPM.gov

Follow us on LinkedIn | X | YouTube

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer; Phillips, Keith; Mitchell, Diana; Hazlett, Amber L.
Subject:	BJELDE, Brian - CLEARED 01/31/2025
Date:	Friday, January 31, 2025 1:28:00 PM
Attachments:	image002.png

**Please note that this cleared message is for a permanent position over 180 days. The individual was previously cleared for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Davis, Melinda M.; Mitchell, Diana; Hazlett, Amber L.; Nickerson, Tiffany V.; Lowe, Dana S.; Dennis, Natasha
Subject: RE: Permanent PIV Request for Brian Bjelde
Date: Thursday, January 30, 2025 8:00:00 AM
Attachments: image002.png

Hi Kim!

We will be reviewing a previous investigation from Brian Bjelde. Nothing further is required at this time. You will receive a separate EOD message.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Wednesday, January 29, 2025 5:00 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Davis, Melinda M. <Melinda.Davis@opm.gov>; Mitchell, Diana <Diana.Mitchell@opm.gov>; Hazlett, Amber L. <Amber.Hazlett@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Dennis, Natasha <Natasha.Dennis@opm.gov>
Subject: Permanent PIV Request for Brian Bjelde

Hi Miranda,

Requesting a permanent PIV for Expert Brain Bjelde. Attached are following documents for your review:

- Resume
- PD
- New Hire Information

Please let me know if you need additional information and/or documents.

Thank you,
Kim

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject:	BOBBA, Akash - CLEARED 01/20/2025
Date:	Monday, January 20, 2025 1:48:00 PM
Attachments:	image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Lowe, Dana S.; Nickerson, Tiffany V.
Subject: RE: Documents for OPM
Date: Monday, January 20, 2025 11:44:00 AM
Attachments: image002.png

Thanks Kim!

We will just need fingerprints for Bobba (which I'm sure he is set to be printed). You will receive a separate EOD message.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Monday, January 20, 2025 11:39 AM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Lowe, Dana S. <Dana.Lowe@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>
Subject: Fw: Documents for OPM

Hi Miranda, here's a hot one

Still trying to figure where this individual will work, I'll send as soon as I can.

V/R
Kim

From: Garcia, Carmen E. <Carmen.Garcia@opm.gov>
Sent: Monday, January 20, 2025 11:11 AM
To: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Subject: Fw: Documents for OPM

Please send to security and I need a folder, label, and a tent for him please

Get Outlook for iOS

From: Garcia, Carmen E.
Sent: Sunday, January 19, 2025 8:22:08 PM

To: Malague, Katie <Katie.Malague@opm.gov>
Subject: FW: Documents for OPM

Hi Katie,

I am not tracking this person. Are you aware of him?

Thanks,
Carmen

From: Akash Bobba <[redacted]>
Sent: Sunday, January 19, 2025 5:22 PM
To: Garcia, Carmen E. <Carmen.Garcia@opm.gov>
Subject: Documents for OPM

> You don't often get email from [redacted]. Learn why this is important

Hi Carmen,

It's great to meet you! I've been told to reach out to you with the following documents for employment at OPM. I have attached them below, please let me know if you need anything else from me.

Thanks,
Akash

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject:	CORISTINE, Edward - CLEARED 01/24/2025
Date:	Friday, January 24, 2025 10:45:00 AM
Attachments:	image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Davis, Melinda M.
To: Beckman, Christopher J.
Cc: Dillaman, Miranda C.
Subject: FW: Rush on Onboarding
Date: Friday, January 24, 2025 7:55:51 AM
Attachments: Outlook-m20yup3t.png
image003.png

Chris-
We have no record fingerprints but we do not have the 306 or release. Kim is supposed to be reaching out this morning to obtain these. That is the latest status we have. As soon as we get the paperwork we can clear. Thanks.

Mindy Davis | Division Director-Personnel Security

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management
M: (202) 386 5095 | OPM.gov
T: (202) 936 2558
OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Hilliard, Everette <Everette.Hilliard@opm.gov>
Sent: Friday, January 24, 2025 5:54 AM
To: Davis, Melinda M. <Melinda.Davis@opm.gov>; Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>; Beckman, Christopher J. <Christopher.Beckman@opm.gov>
Subject: Fwd: Rush on Onboarding

Sent from my iPhone

Begin forwarded message:

From: "Garcia, Carmen E." <Carmen.Garcia@opm.gov>
Date: January 23, 2025 at 10:07:38 PM EST
To: "Ezell, Charles E." <Charles.Ezell@opm.gov>, "Hilliard, Everette" <Everette.Hilliard@opm.gov>
Cc: "Bjelde, Brian" <Brian.Bjelde@opm.gov>
Subject: Re: Rush on Onboarding

Good Evening Acting Director,

I will prioritize this and make sure we see this through expeditiously. We just need to execute an MOU and it's drafted and signed on our end. I just need to get in touch with their respective agencies for their signature in order to finalize the detail.

We hope to have resolution early tomorrow.

Thank you,
Carmen

Get Outlook for iOS

From: Ezell, Charles E. <Charles.Ezell@opm.gov>
Sent: Thursday, January 23, 2025 10:04:32 PM
To: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Hilliard, Everette <Everette.Hilliard@opm.gov>
Cc: Bjelde, Brian <Brian.Bjelde@opm.gov>
Subject: Rush on Onboarding

Reid & Carmen, we need to quickly onboard the two DOGE employees tomorrow if at all possible. I'm not sure where they are in the process but we are desperately needing their engineering skills to help with a special project for President Trump.

- Edward Coristine
- Nikhil Rajpal

.ce

Chuck Ezell

Acting Director

U.S. Office of Personnel Management

(478) 832-8119

Charles.Ezell@opm.gov

OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject:	HOGAN, Gregory - CLEARED 01/14/2025
Date:	Tuesday, January 14, 2025 12:18:00 PM
Attachments:	image002.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From:	Dillaman, Miranda C.
To:	Sylke, Kimberly D.
Cc:	Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Pettit, John; Lowe, Dana S.; Nickerson, Tiffany V.
Subject:	RE: New Hire Information for Incoming Senior Advisor to the Director (Hogan)
Date:	Monday, January 13, 2025 2:35:00 PM
Attachments:	image003.png image002.png

Hi Kim!

Greg Hogan will need fingerprints (which I have been notified he came in for fingerprinting today). You will receive a separate EOD message.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Monday, January 13, 2025 2:03 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Beckman, Christopher J. <Christopher.Beckman@opm.gov>; Davis, Melinda M. <Melinda.Davis@opm.gov>; Pettit, John <John.Pettit@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>
Subject: New Hire Information for Incoming Senior Advisor to the Director (Hogan)

Good Afternoon Miranda,

Requesting temporary clearance (less than 180 days) for Greg Hogan, incoming Senior Advisor to the Director. Attached are the required documents for your review.

Please let me know if you need any additional information or have any questions.

V/R

Kim

Kim Sylke (pronouns: she/her)

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) 936-3339

Email: kimberly.sylke@opm.gov

OPM.gov

Follow us on LinkedIn | X | YouTube

Stugart, Sarah B.

From: Stugart, Sarah B.
Sent: Thursday, March 6, 2025 2:10 PM
To: Hogan, Greg
Subject: Clearance-Hogan

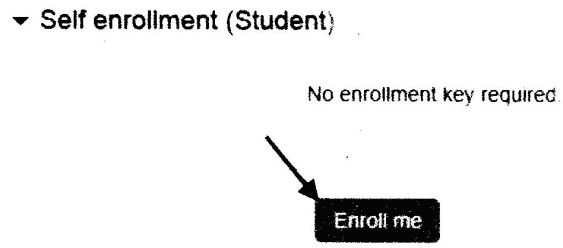
Importance: High

Good afternoon, Mr. Hogan,

As part of your duties with USOPM, it has been requested that you be granted access to Top Secret classified information. Additionally, it was further requested that you be processed for SCI access. The Top-Secret access is required to be granted prior to the SCI access and this email informs you of the requirements for the Top-Secret clearance access only. Once the Top-Secret clearance is in place you will be provided further instructions for the SCI access.

You are required to complete the on-line Classified National Security Awareness and Insider Threat Training located on the USOPM Learning Connection portal. The link to the training is: https://learningconnection.opm.gov/course/view.php?id=32655 Chrome Browser is recommended.

Access the OPM Learning Connection web site and locate the course. Directly below the course title will be an **Enroll Me** button that will allow you to self-enroll (see screen shot below). Once you click that button, you will receive an email stating that you are enrolled. You do not have to open the email or do anything with it. You should be able to click on the course's link to enter the training modules.



*If you do not see any of the above steps when you log on do a key word search for the course by typing or copying and pasting the following into the course search box: **CY 2024 Classified National Security Information Awareness and Insider Threat Training.** The course should now be displayed for you to choose.
You must complete the on-line training and pass it with a score of at least 80. After you complete the training, you must print your certificate. If you cannot obtain the certificate, please obtain a copy/snapshot of the actual test results. Send me a copy of your certificate/test results by email attachment to sarah.stugart@opm.gov. Upon receipt of the certificate, arrangements will be made to complete the SF 312, Classified Information Nondisclosure Agreement.

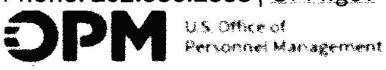
If you encounter any technical difficulties with the OPM Learning Connection, please refer to the website itself for instructions on how to contact the Help Desk.

If you have any questions regarding the clearance process, please let me know. Thank you.

Thank you.

Sarah Stugart | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
Phone: 202.936.2588 | OPM.gov



Follow us on LinkedIn | Twitter | YouTube

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIONS SERVICE
WASHINGTON, DC 20415

CERTIFICATION OF INVESTIGATION

DATE: 03/05/2025

SUBMITTING OFFICE: SON - 133H SECURITY OFFICE: SOI - OM00

OPM
ATTN: CSEA
P.O. BOX 618
1137 BRANCHTON ROAD
BOYERS, PA 16018

NAME: HOGAN, GREGORY JOHN

SSN: [redacted] DOB [redacted] POSITION: CHIEF INFORMATION OF

CASE TYPE: T5 CLOSING DATE: 03/05/2025 OPM CASE #: 2509900333
EXTRA COVERAGE: L / BVS
3 / ADVANCED REPORT OF NAC
PT / PRESIDENTIAL TRANSITION CASES
POSITION CODE : /

SCHEDULED DATE: 02/06/2025

INVESTIGATION CONDUCTED FROM: SF86 (7/17)

THIS CERTIFIES THAT A BACKGROUND INVESTIGATION ON THE PERSON IDENTIFIED ABOVE HAS BEEN COMPLETED. THE RESULTS OF THIS INVESTIGATION WERE SENT TO THE SECURITY OFFICE FOR A SECURITY/SUITABILITY DETERMINATION.

****

AGENCY CERTIFICATION: THE RESULTS OF THIS INVESTIGATION HAVE BEEN REVIEWED, AND A FINAL DETERMINATION HAS BEEN MADE.

AGENCY CERTIFYING OFFICIAL SARA ARBLASTER Digitally signed by SARA ARBLASTER Date: 2025.03.06 11:46:16 -05'00' DATE

FILE THIS CERTIFICATE ON THE PERMANENT SIDE OF THE PERSON'S OFFICIAL PERSONNEL FOLDER AFTER THE FINAL AGENCY DETERMINATION IS MADE.

Personnel Security Group

From: Personnel Security Group
Sent: Thursday, March 6, 2025 12:55 PM
To: Hogan, Greg
Subject: Hogan, Gregory - NOTIFICATION OF COMPLETION OF INVESTIGATIVE PROCESS

Congratulations Mr. Hogan,

The background investigation for your employment with the U.S. Office of Personnel Management was favorably adjudicated by Personnel Security on March 6, 2025. Your investigation was favorably adjudicated under both 5 CFR 731, Suitability Guidelines and E.O. 12968, National Security Adjudicative Guidelines. If your position requires access to classified information, you are eligible to be processed for a security clearance equivalent to your Position Designation. You will be contacted separately by a member of the Personnel Security Staff to complete a security clearance briefing/training and to execute the SF 312 Non-disclosure Agreement prior to being granted access to classified information. If you have any questions regarding this notice or any other Personnel Security related matter, please contact me at the number below.

On October 1, 2019, as authorized by Executive Order 13869, the mission, records, and personnel of the OPM, National Background Investigations Bureau, transferred to the Department of Defense, Defense Counterintelligence and Security Agency (DCSA). Accordingly, as of October 1, 2019, in order to obtain a copy of your background investigation, request an amendment to your records, or file a FOIA request related to background investigation data or records, please follow the instructions at DCSA's website: https://www.dcsa.mil/mc/pv/mbi/mr/. If you have specific questions, you may contact the DCSA Freedom of Information and Privacy Office for Investigations at: (878)274-1185.

Thank you,

Sara Arblaster
Personnel Security Specialist
U.S. Office of Personnel Management
Facilities, Security & Emergency Management-Personnel Security
o: (202)936-1292
f: (724)738-0278
sara.arblaster@opm.gov
OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer; Hazlett, Amber L.; Mitchell, Diana
Subject:	HOGAN, Gregory - CLEARED 02/10/2025
Date:	Monday, February 10, 2025 1:12:00 PM
Attachments:	image002.png

**Please note that this cleared message is for a permanent position over 180 days. The individual was previously cleared for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From:	Dillaman, Miranda C.
To:	Sylke, Kimberly D.
Cc:	Davis, Melinda M.; Mitchell, Diana; Hazlett, Amber L.; Nickerson, Tiffany V.; Lowe, Dana S.; Dennis, Natasha
Subject:	RE: Permanent - Greg Hogan (Noncareer SES) - Chief Information Officer
Date:	Thursday, January 30, 2025 6:14:00 AM
Attachments:	image002.png

Hi Kim!

Greg Hogan will need a full investigation on the 86. Fingerprints are not needed. I will take care of the eApp, email and cc you.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Wednesday, January 29, 2025 4:07 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Davis, Melinda M. <Melinda.Davis@opm.gov>; Mitchell, Diana <Diana.Mitchell@opm.gov>; Hazlett, Amber L. <Amber.Hazlett@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Dennis, Natasha <Natasha.Dennis@opm.gov>
Subject: Permanent - Greg Hogan (Noncareer SES) - Chief Information Officer

Hi Miranda,

Requesting clearance to move Greg Hogan to a permeant Chief Information Officer (Noncareer SES) position. Attached are following documents for your review:

- Resume
- PD
- New Hire Information

Please let me know if you need additional information.

V/R
Kim

APPLICANT INFORMATION - Page 2

Enrollment ID [redacted] **Name** HOGAN GREGORY JOHN **DOB** [redacted]

ADJUDICATION INFORMATION

Adjudication Status ADJUDICATED

Adjudication Create Date / Last Update 10-Feb-2025 13:12 / 07-Mar-2025 12:53

NCHC/FBI APPROVED **NCHC/FBI Adjudicator ID** [redacted]

NACI APPROVED **NACI Adjudicator ID** [redacted]

Adj Last Update Agency OFFICE OF PERSONNEL MANAGEMENT

Adj Last Update Agency Date 07-Mar-2025 12:53

PIV Agency Specific Criteria Status **PIV-I Agency Specific Criteria Status**

PIV Agency Specific Criteria Date **PIV-I Agency Specific Criteria Date**

ENROLLMENT INFORMATION

Enrollment Status COMPLETE **Last Enrollment Date** 10-Feb-2025 16:23

Enrollment Create Date 10-Feb-2025 13:12 **Enrollment Last Update** 10-Feb-2025 16:22

Document Referral NO

Enrollment Site ID/Description 102415 / OPM LCS 10

Enrollment Site Address: Line 1 1H17

Line 2 1900 E ST NW

Line 3

City /State / Zip Code WASHINGTON / DC / 20415

ISSUANCE INFORMATION

CURRENT CARD

Issuance Status ACTIVE

Create/Last Update Date 12-Feb-2025 16:33 / 13-Feb-2025 9:37

CMS Card ID [redacted]

Card ID 2 **Card Destroyed** NO

FASC-N [redacted]

Card UUID [redacted]

Issuance Sub-Status ACTIVATED

Issuance Cred Option PIV

Certificate Set 4

Card Profile V8.1

REPLACEMENT CARD

Issuance Status NO STATUS

Create/Last Update Date /

CMS Card ID

Card ID

FASC-N

Card UUID

Issuance Sub-Status NO STATUS

Issuance Cred Option

Certificate Set

Card Profile

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Facilities, Security and
Emergency Management

February 10, 2025

MEMORANDUM FOR Jennifer Duncan
Chief, Adjudications and Compliance
Personnel Security

FROM: Miranda Dillaman
Personnel Security Specialist
Facilities, Security & Emergency Management

Subject: Waiver of Pre-Appointment Background Investigation Requirements for,Appointment to Special-Sensitive Positions

This is a request for a waiver of the pre-appointment background investigation requirements for Gregory Hogan's appointment to a special-sensitive position. This individual has been selected for the position of Chief Information Officer with the Office of the Chief Information Officer.

Executive Order 10450, "Security Requirements for Government Employment", Executive Order 12968, "Access to Classified Information", and Security Executive Agent Directive 8, (SEAD 8) provide that in exceptional circumstances or in an emergency, when official functions must be performed prior to the completion of the investigation and adjudication process or when in the national interest, an individual may be appointed on a temporary basis to a special-sensitive position prior to the investigation's completion. A delay in appointment would be harmful to national security and adversely impact the organization's mission.

Upon approval, the U.S. Office of Personnel Management's (OPM's) Personnel Security will initiate the above-named individual's personal security package for an expedited background investigation and pre-waiver checks, as appropriate. It is in the Agency's best interest to affect this appointment as soon as possible.

(Note: A waiver cannot be issued unless mandated portions of the current Tier 5 have been favorably reviewed.)

DECISION:
☒Approved ☐Not Approved ☐Let's Discuss

2/10/2025

X Jennifer Duncan
Branch Chief, OPM-FSEM-Personnel Security

Signed by: Office of Personnel Management

OPM U.S. Office of Personnel Management

This is to certify that

Gregory Hogan

has completed the course

CY 2024 Classified National Security Information Awareness and Insider Threat Training

March 9, 2025

Tierra F. Elsey

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject:	KLIGER, Gavin - CLEARED 01/14/2025
Date:	Tuesday, January 14, 2025 12:25:00 PM
Attachments:	image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From:	Dillaman, Miranda C.
To:	Sylke, Kimberly D.
Cc:	Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Pettit, John; Lowe, Dana S.; Nickerson, Tiffany V.
Subject:	RE: New Hire Information for Incoming Senior Advisor to the Director for Technology & Delivery Kliger
Date:	Monday, January 13, 2025 2:23:00 PM
Attachments:	image003.png image001.png

Hi Kim!

Gavin will need fingerprints (which I have been notified he came in for fingerprinting today). You will receive a separate EOD message.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Monday, January 13, 2025 1:50 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Beckman, Christopher J. <Christopher.Beckman@opm.gov>; Davis, Melinda M. <Melinda.Davis@opm.gov>; Pettit, John <John.Pettit@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>
Subject: New Hire Information for Incoming Senior Advisor to the Director for Technology & Delivery Kliger

Good Afternoon Miranda,

Requesting temporary clearance (less than 180 days) for Gavin Klinger, incoming Senior Advisor to the Director. Attached are the required documents for your review.

Please let me know if you need any additional information or have any questions.

V/R

Kim

Kim Sylke (pronouns: she/her)

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) 936-3339

Email: kimberly.sylke@opm.gov

OPM.gov

Follow us on LinkedIn | X | YouTube

Weaver, Tyler R.

From: Weaver, Tyler R.
Sent: Wednesday, April 2, 2025 12:07 PM
To: Kliger, Gavin
Cc: Kennedy, Shellie L; Hicks, John A; Stugart, Sarah B.
Subject: Kliger, Gavin - Top Secret/SCI Clearance Request

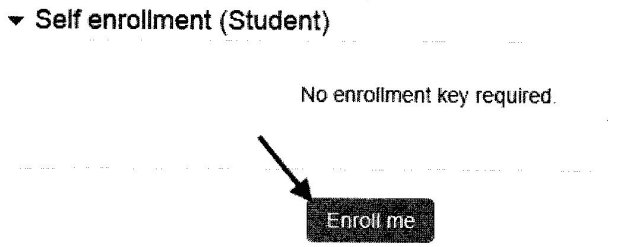
Importance: High

Good afternoon Gavin,

As part of your duties with USOPM, it has been requested that you be granted access to Top Secret classified information. Additionally, it was further requested that you be processed for SCI access. The Top-Secret access is required to be granted prior to the SCI access and this email informs you of the requirements for the Top-Secret clearance access only. Once the Top-Secret clearance is in place you will be provided further instructions for the SCI access.

You are required to complete the on-line Classified National Security Awareness and Insider Threat Training located on the USOPM Learning Connection portal. The link to the training is: https://learningconnection.opm.gov/course/view.php?id=32655 Chrome Browser is recommended.

Access the OPM Learning Connection web site and locate the course. Directly below the course title will be an **Enroll Me** button that will allow you to self-enroll (see screen shot below). Once you click that button, you will receive an email stating that you are enrolled. You do not have to open the email or do anything with it. You should be able to click on the course's link to enter the training modules.



*If you do not see any of the above steps when you log on do a key word search for the course by typing or copying and pasting the following into the course search box: **CY 2024 Classified National Security Information Awareness and Insider Threat Training.** The course should now be displayed for you to choose.

You must complete the on-line training and pass it with a score of at least 80. After you complete the training, you must print your certificate. If you cannot obtain the certificate, please obtain a copy/snapshot of the actual test results. Send me a copy of your certificate/test results by email attachment to Tyler.Weaver@opm.gov. Upon receipt of the certificate, arrangements will be made to complete the SF 312, Classified Information Nondisclosure Agreement.

If you encounter any technical difficulties with the OPM Learning Connection, please refer to the website itself for instructions on how to contact the Help Desk.

If you have any questions regarding the clearance process, please let me know.

Thank you!

Tyler Weaver | Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
OPM.gov

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer; Hazlett, Amber L.; Mitchell, Diana
Subject:	KLIGER, Gavin - CLEARED 02/18/2025
Date:	Tuesday, February 18, 2025 12:46:00 PM
Attachments:	image001.png

**Please note that this cleared message is for a permanent position over 180 days. The individual was previously cleared for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Davis, Melinda M.; Mitchell, Diana; Hazlett, Amber L.; Nickerson, Tiffany V.; Lowe, Dana S.; Dennis, Natasha
Subject: RE: Gavin Kliger (Schedule C) - Senior Advisor to the Director
Date: Thursday, January 30, 2025 7:24:00 AM
Attachments: image002.png

Hi Kim!

Gavin Kliger will need a full investigation on the 86. Fingerprints are not needed. I will take care of the eApp, email and cc you.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Wednesday, January 29, 2025 4:28 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Davis, Melinda M. <Melinda.Davis@opm.gov>; Mitchell, Diana <Diana.Mitchell@opm.gov>; Hazlett, Amber L. <Amber.Hazlett@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Dennis, Natasha <Natasha.Dennis@opm.gov>
Subject: Gavin Kliger (Schedule C) - Senior Advisor to the Director

Hi Miranda,

Requesting clearance to move Gavin Kliger to a Senior Advisor to the Director (Schedule C) position permanently. Attached are following documents for your review:

- Resume
- PD
- New Hire Information

Please let me know if you need additional information.

V/R
Kim

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIONS SERVICE
WASHINGTON, DC 20415

CERTIFICATION OF INVESTIGATION

DATE: 03/18/2025

SUBMITTING OFFICE: SON - 133H SECURITY OFFICE: SOI - OM00

OPM
ATTN: CSEA
P.O. BOX 618
1137 BRANCHTON ROAD
BOYERS, PA 16018

NAME: KLIGER, GAVIN IAN

SSN: [redacted] DOB: [redacted] POSITION: SENIOR ADVISOR TO TH

CASE TYPE: T5 CLOSING DATE: 03/18/2025 OPM CASE #: 2509900345
EXTRA COVERAGE: L / BVS
3 / ADVANCED REPORT OF NAC
PT / PRESIDENTIAL TRANSITION CASES
POSITION CODE : /

SCHEDULED DATE: 02/07/2025

INVESTIGATION CONDUCTED FROM: SF86 (7/17)

THIS CERTIFIES THAT A BACKGROUND INVESTIGATION ON THE PERSON IDENTIFIED ABOVE HAS BEEN COMPLETED. THE RESULTS OF THIS INVESTIGATION WERE SENT TO THE SECURITY OFFICE FOR A SECURITY/SUITABILITY DETERMINATION.

****

AGENCY CERTIFICATION: THE RESULTS OF THIS INVESTIGATION HAVE BEEN REVIEWED, AND A FINAL DETERMINATION HAS BEEN MADE.

AGENCY CERTIFYING OFFICIAL SARA ARBLASTER Digitally signed by SARA ARBLASTER Date: 2025.03.21 14:39:02 -04'00' DATE

FILE THIS CERTIFICATE ON THE PERMANENT SIDE OF THE PERSON'S OFFICIAL PERSONNEL FOLDER AFTER THE FINAL AGENCY DETERMINATION IS MADE.

Personnel Security Group

From: Personnel Security Group
Sent: Friday, March 21, 2025 2:54 PM
To: Kliger, Gavin
Subject: Kliger, Gavin - NOTIFICATION OF COMPLETION OF INVESTIGATIVE PROCESS

Congratulations Mr. Kliger,

The background investigation for your employment with the U.S. Office of Personnel Management was favorably adjudicated by Personnel Security on March 21, 2025. Your investigation was favorably adjudicated under both 5 CFR 731, Suitability Guidelines and E.O. 12968, National Security Adjudicative Guidelines. If your position requires access to classified information, you are eligible to be processed for a security clearance equivalent to your Position Designation. In order to complete the security clearance process, you will need to be nominated by your Division Director utilizing the OPM Form 1680 (Issuance of a Security Clearance) which can be requested from FSEM Personnel Security. If you have any questions regarding this notice or any other Personnel Security related matter, please contact me at the number below.

On October 1, 2019, as authorized by Executive Order 13869, the mission, records, and personnel of the OPM, National Background Investigations Bureau, transferred to the Department of Defense, Defense Counterintelligence and Security Agency (DCSA). Accordingly, as of October 1, 2019, in order to obtain a copy of your background investigation, request an amendment to your records, or file a FOIA request related to background investigation data or records, please follow the instructions at DCSA's website: https://www.dcsa.mil/mc/pv/mbi/mr/. If you have specific questions, you may contact the DCSA Freedom of Information and Privacy Office for Investigations at: (878)274-1185.

Thank you,

Sara Arblaster
Personnel Security Specialist
U.S. Office of Personnel Management
Facilities, Security & Emergency Management-Personnel Security
o: (202)936-1292
f: (724)738-0278
sara.arblaster@opm.gov
OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Facilities, Security and
Emergency Management

February 18, 2025

MEMORANDUM FOR Jennifer Duncan
Chief, Adjudications and Compliance
Personnel Security

FROM: Miranda Dillaman
Personnel Security Specialist
Facilities, Security & Emergency Management

Subject: Waiver of Pre-Appointment Background Investigation Requirements for Appointment to Critical-Sensitive Positions

This is a request for a waiver of the pre-appointment background investigation requirements for Gavin Kliger's appointment to a critical-sensitive position. This individual has been selected for the position of Senior Advisor to the Director of Information Technology with the Office of the Director.

Executive Order 10450, "Security Requirements for Government Employment", Executive Order 12968, "Access to Classified Information", and Security Executive Agent Directive 8, (SEAD 8) provide that in exceptional circumstances or in an emergency, when official functions must be performed prior to the completion of the investigation and adjudication process or when in the national interest, an individual may be appointed on a temporary basis to a critical-sensitive position prior to the investigation's completion. A delay in appointment would be harmful to national security and adversely impact the organization's mission.

Upon approval, the U.S. Office of Personnel Management's (OPM's) Personnel Security will initiate the above-named individual's personal security package for an expedited background investigation and pre-waiver checks, as appropriate. It is in the Agency's best interest to affect this appointment as soon as possible.

(Note: A waiver cannot be issued unless mandated portions of the current Tier 5 have been favorably reviewed.)

DECISION:
☒Approved ☐Not Approved ☐Let's Discuss

X
Branch Chief, OPM-FSEM-Personnel Security

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject:	RAJPAL, Nikhil - CLEARED 01/24/2025
Date:	Friday, January 24, 2025 10:46:00 AM
Attachments:	image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Davis, Melinda M.
To: Beckman, Christopher J.
Cc: Dillaman, Miranda C.
Subject: FW: Rush on Onboarding
Date: Friday, January 24, 2025 7:55:51 AM
Attachments: Outlook-m20yup3t.png
image003.png

Chris-
We have no record fingerprints but we do not have the 306 or release. Kim is supposed to be reaching out this morning to obtain these. That is the latest status we have. As soon as we get the paperwork we can clear. Thanks.

Mindy Davis | Division Director-Personnel Security

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management
M: (202) 386 5095 | OPM.gov
T: (202) 936 2558
OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Hilliard, Everette <Everette.Hilliard@opm.gov>
Sent: Friday, January 24, 2025 5:54 AM
To: Davis, Melinda M. <Melinda.Davis@opm.gov>; Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>; Beckman, Christopher J. <Christopher.Beckman@opm.gov>
Subject: Fwd: Rush on Onboarding

Sent from my iPhone

Begin forwarded message:

From: "Garcia, Carmen E." <Carmen.Garcia@opm.gov>
Date: January 23, 2025 at 10:07:38 PM EST
To: "Ezell, Charles E." <Charles.Ezell@opm.gov>, "Hilliard, Everette" <Everette.Hilliard@opm.gov>
Cc: "Bjelde, Brian" <Brian.Bjelde@opm.gov>
Subject: Re: Rush on Onboarding

Good Evening Acting Director,

I will prioritize this and make sure we see this through expeditiously. We just need to execute an MOU and it's drafted and signed on our end. I just need to get in touch with their respective agencies for their signature in order to finalize the detail.

We hope to have resolution early tomorrow.

Thank you,
Carmen

Get Outlook for iOS

From: Ezell, Charles E. <Charles.Ezell@opm.gov>
Sent: Thursday, January 23, 2025 10:04:32 PM
To: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Hilliard, Everette <Everette.Hilliard@opm.gov>
Cc: Bjelde, Brian <Brian.Bjelde@opm.gov>
Subject: Rush on Onboarding

Reid & Carmen, we need to quickly onboard the two DOGE employees tomorrow if at all possible. I'm not sure where they are in the process but we are desperately needing their engineering skills to help with a special project for President Trump.

- Edward Coristine
- Nikhil Rajpal

.ce

Chuck Ezell

Acting Director

U.S. Office of Personnel Management

(478) 832-8119

Charles.Ezell@opm.gov

OPM.gov

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer
Subject:	SULLIVAN, James - CLEARED 01/14/2025
Date:	Tuesday, January 14, 2025 6:05:00 PM
Attachments:	image001.png

Please note that this cleared message is for a temporary appointment for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From:	Dillaman, Miranda C.
To:	Sylke, Kimberly D.
Cc:	Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Lowe, Dana S.
Subject:	RE: New Hire Information for Incoming Senior Advisor to the Director (Sullivan)
Date:	Tuesday, January 14, 2025 3:42:00 PM
Attachments:	image004.png image005.png image001.png

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Tuesday, January 14, 2025 3:30 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Beckman, Christopher J. <Christopher.Beckman@opm.gov>; Davis, Melinda M. <Melinda.Davis@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>
Subject: Re: New Hire Information for Incoming Senior Advisor to the Director (Sullivan)

Hi Miranda, updated 306 attached.

V/R
Kim

From: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Sent: Monday, January 13, 2025 2:40 PM
To: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Cc: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Beckman, Christopher J. <Christopher.Beckman@opm.gov>; Davis, Melinda M. <Melinda.Davis@opm.gov>; Pettit, John <John.Pettit@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>
Subject: RE: New Hire Information for Incoming Senior Advisor to the Director (Sullivan)

Hi Kim!

Jamie Sullivan will need fingerprints (which I have been notified Jamie came in for fingerprinting today). Would you mind having Jamie submit a new 306? The answers to the questions aren't

populating and the date signed isn't correct.

You will receive a separate EOD message.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Monday, January 13, 2025 2:13 PM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Garcia, Carmen E. <Carmen.Garcia@opm.gov>; Beckman, Christopher J. <Christopher.Beckman@opm.gov>; Davis, Melinda M. <Melinda.Davis@opm.gov>; Pettit, John <John.Pettit@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>
Subject: New Hire Information for Incoming Senior Advisor to the Director (Sullivan)

Good Afternoon Miranda,

Requesting temporary clearance (less than 180 days) for Jamie Sullivan, incoming Senior Advisor to the Director. Attached are the required documents for your review.

Please let me know if you need any additional information or have any questions.

V/R

Kim

Kim Sylke (pronouns: she/her)

SUPERVISORY HR SPECIALIST, EXECUTIVE RESOURCES

Office of the Chief Human Capital Officer | U.S. Office of Personnel Management

1900 E. St. NW | Washington DC 20415

Office: (202) 936-3339

Email: kimberly.sylke@opm.gov

OPM.gov

Follow us on LinkedIn | X | YouTube

Stugart, Sarah B.

From: Stugart, Sarah B.
Sent: Tuesday, March 4, 2025 1:54 PM
To: Sullivan, James D.
Subject: Clearance- Sullivan

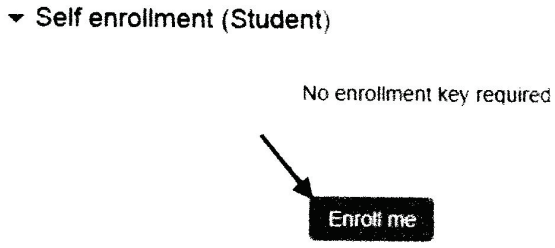
Importance: High

Good afternoon, Mr. Sullivan,

As part of your duties with USOPM, it has been requested that you be granted access to Top Secret classified information. Additionally, it was further requested that you be processed for SCI access. The Top-Secret access is required to be granted prior to the SCI access and this email informs you of the requirements for the Top-Secret clearance access only. Once the Top-Secret clearance is in place you will be provided further instructions for the SCI access.

You are required to complete the on-line Classified National Security Awareness and Insider Threat Training located on the USOPM Learning Connection portal. The link to the training is: https://learningconnection.opm.gov/course/view.php?id=32655 Chrome Browser is recommended.

Access the OPM Learning Connection web site and locate the course. Directly below the course title will be an **Enroll Me** button that will allow you to self-enroll (see screen shot below). Once you click that button, you will receive an email stating that you are enrolled. You do not have to open the email or do anything with it. You should be able to click on the course's link to enter the training modules.



*If you do not see any of the above steps when you log on do a key word search for the course by typing or copying and pasting the following into the course search box: **CY 2024 Classified National Security Information Awareness and Insider Threat Training.** The course should now be displayed for you to choose.
You must complete the on-line training and pass it with a score of at least 80. After you complete the training, you must print your certificate. If you cannot obtain the certificate, please obtain a copy/snapshot of the actual test results. Send me a copy of your certificate/test results by email attachment to sarah.stugart@opm.gov. Upon receipt of the certificate, arrangements will be made to complete the SF 312, Classified Information Nondisclosure Agreement.

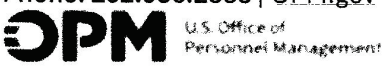
If you encounter any technical difficulties with the OPM Learning Connection, please refer to the website itself for instructions on how to contact the Help Desk.

If you have any questions regarding the clearance process, please let me know. Thank you.

Thank you.

Sarah Stugart | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
Phone: 202.936.2588 | OPM.gov



Follow us on LinkedIn | Twitter | YouTube

Personnel Security Group

From: Personnel Security Group
Sent: Tuesday, March 4, 2025 11:26 AM
To: Sullivan, James D.
Subject: Sullivan, James - NOTIFICATION OF COMPLETION OF INVESTIGATIVE PROCESS

Congratulations Mr. Sullivan,

The background investigation for your employment with the U.S. Office of Personnel Management was favorably adjudicated by Personnel Security on March 4, 2025. Your investigation was favorably adjudicated under both 5 CFR 731, Suitability Guidelines and E.O. 12968, National Security Adjudicative Guidelines. If your position requires access to classified information, you are eligible to be processed for a security clearance equivalent to your Position Designation. In order to complete the security clearance process, the OPM Form 1680 (Issuance of a Security Clearance) has been submitted and you will be contacted separately by a member of the Personnel Security Staff to complete a security clearance briefing/training and to execute the SF 312 Non-disclosure Agreement prior to being granted access to classified information. If you have any questions regarding this notice or any other Personnel Security related matter, please contact me at the number below.

On October 1, 2019, as authorized by Executive Order 13869, the mission, records, and personnel of the OPM, National Background Investigations Bureau, transferred to the Department of Defense, Defense Counterintelligence and Security Agency (DCSA). Accordingly, as of October 1, 2019, in order to obtain a copy of your background investigation, request an amendment to your records, or file a FOIA request related to background investigation data or records, please follow the instructions at DCSA's website: https://www.dcsa.mil/mc/pv/mbi/mr/. If you have specific questions, you may contact the DCSA Freedom of Information and Privacy Office for Investigations at: (878)274-1185.

Thank you,

Sara Arblaster
Personnel Security Specialist
U.S. Office of Personnel Management
Facilities, Security & Emergency Management-Personnel Security
o: (202)936-1292
f: (724)738-0278
sara.arblaster@opm.gov
OPM.gov

Follow us on LinkedIn | Twitter | YouTube

From:	Personnel Security Group
To:	Sylke, Kimberly D.
Cc:	Lowe, Dana S.; Nickerson, Tiffany V.; Garcia, Carmen E.; Beckman, Christopher J.; Davis, Melinda M.; Duncan, Jennifer; Hazlett, Amber L.; Mitchell, Diana
Subject:	SULLIVAN, James - CLEARED 02/12/2025
Date:	Wednesday, February 12, 2025 1:46:00 PM
Attachments:	image001.png

**Please note that this cleared message is for a permanent position over 180 days. The individual was previously cleared for less than 180 days.

Thank you!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Dillaman, Miranda C.
To: Sylke, Kimberly D.
Cc: Davis, Melinda M.; Mitchell, Diana; Hazlett, Amber L.; Nickerson, Tiffany V.; Lowe, Dana S.; Dennis, Natasha
Subject: RE: James Sullivan (Schedule C) - Senior Advisor
Date: Thursday, January 30, 2025 5:03:00 PM
Attachments: image002.png

Hi Kim!

James Sullivan will need a full investigation on the 86. Fingerprints are not needed. I will take care of the eApp, email and cc you.

Thanks!

Miranda Dillaman | Senior Personnel Security Specialist

U.S. Office of Personnel Management
Office of Facilities, Security, and Emergency Management | Personnel Security
T: (202) 936-2538 | OPM.gov

OPM U.S. Office of Personnel Management

Follow us on LinkedIn | Twitter | YouTube

From: Sylke, Kimberly D. <Kimberly.Sylke@opm.gov>
Sent: Thursday, January 30, 2025 10:22 AM
To: Dillaman, Miranda C. <Miranda.Dillaman@opm.gov>
Cc: Davis, Melinda M. <Melinda.Davis@opm.gov>; Mitchell, Diana <Diana.Mitchell@opm.gov>; Hazlett, Amber L. <Amber.Hazlett@opm.gov>; Nickerson, Tiffany V. <Tiffany.Nickerson@opm.gov>; Lowe, Dana S. <Dana.Lowe@opm.gov>; Dennis, Natasha <Natasha.Dennis@opm.gov>
Subject: James Sullivan (Schedule C) - Senior Advisor

Good Morning Miranda,

Requesting clearance to move James Sullivan to a Senior Advisor (Schedule C) position permanently. Attached are following documents for your review:

- Resume
- PD *(This is a new PD, so it doesn't have a position designation record yet.)*
- New Hire Information

Please let me know if you need additional information.

V/R
Kim

APPLICANT INFORMATION - Page 2

Enrollment ID [redacted] **Name** SULLIVAN III JAMES DANIEL **DOB** [redacted]

ADJUDICATION INFORMATION

Adjudication Status ADJUDICATED

Adjudication Create Date / Last Update 12-Feb-2025 13:50 / 04-Mar-2025 11:40

NCHC/FBI APPROVED **NCHC/FBI Adjudicator ID** [redacted]

NACI APPROVED **NACI Adjudicator ID** [redacted]

Adj Last Update Agency OFFICE OF PERSONNEL MANAGEMENT

Adj Last Update Agency Date 04-Mar-2025 11:40

PIV Agency Specific Criteria Status **PIV-I Agency Specific Criteria Status**

PIV Agency Specific Criteria Date **PIV-I Agency Specific Criteria Date**

ENROLLMENT INFORMATION

Enrollment Status COMPLETE **Last Enrollment Date** 14-Feb-2025 9:43

Enrollment Create Date 12-Feb-2025 13:50 **Enrollment Last Update** 14-Feb-2025 9:43

Document Referral NO

Enrollment Site ID/Description 102415 / OPM LCS 10

Enrollment Site Address: Line 1 1H17

Line 2 1900 E ST NW

Line 3

City /State / Zip Code WASHINGTON / DC / 20415

ISSUANCE INFORMATION

CURRENT CARD

Issuance Status ACTIVE

Create/Last Update Date 12-Feb-2025 13:50 / 25-Feb-2025 16:26

CMS Card ID [redacted]

Card ID 1 **Card Destroyed** NO

FASC-N [redacted]

Card UUID [redacted]

Issuance Sub-Status ACTIVATED

Issuance Cred Option PIV

Certificate Set 4

Card Profile V8.1

REPLACEMENT CARD

Issuance Status NO STATUS

Create/Last Update Date /

CMS Card ID

Card ID

FASC-N

Card UUID

Issuance Sub-Status NO STATUS

Issuance Cred Option

Certificate Set

Card Profile

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
INVESTIGATIONS SERVICE
WASHINGTON, DC 20415

CERTIFICATION OF INVESTIGATION

DATE: 03/03/2025

SUBMITTING OFFICE: SON - 133H SECURITY OFFICE: SOI - OM00

OPM
ATTN: CSEA
P.O. BOX 618
1137 BRANCHTON ROAD
BOYERS, PA 16018

NAME: SULLIVAN, JAMES DANIEL III

SSN: [redacted] DOB [redacted] POSITION: SENIOR ADVISOR - PRE

CASE TYPE: T5 CLOSING DATE: 03/03/2025 OPM CASE #: 2509900384
EXTRA COVERAGE: L / BVS
3 / ADVANCED REPORT OF NAC
PT / PRESIDENTIAL TRANSITION CASES
POSITION CODE : /

SCHEDULED DATE: 02/11/2025

INVESTIGATION CONDUCTED FROM: SF86 (7/17)

THIS CERTIFIES THAT A BACKGROUND INVESTIGATION ON THE PERSON IDENTIFIED ABOVE HAS BEEN COMPLETED. THE RESULTS OF THIS INVESTIGATION WERE SENT TO THE SECURITY OFFICE FOR A SECURITY/SUITABILITY DETERMINATION.

****

AGENCY CERTIFICATION: THE RESULTS OF THIS INVESTIGATION HAVE BEEN REVIEWED, AND A FINAL DETERMINATION HAS BEEN MADE.

AGENCY CERTIFYING OFFICIAL SARA ARBLASTER Digitally signed by SARA ARBLASTER Date: 2025.03.04 10:44:24 -05'00' DATE

FILE THIS CERTIFICATE ON THE PERMANENT SIDE OF THE PERSON'S OFFICIAL PERSONNEL FOLDER AFTER THE FINAL AGENCY DETERMINATION IS MADE.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Facilities, Security and
Emergency Management

February 12, 2025

MEMORANDUM FOR Jennifer Duncan
Chief, Adjudications and Compliance
Personnel Security

FROM: Miranda Dillaman
Personnel Security Specialist
Facilities, Security & Emergency Management

Subject: Waiver of Pre-Appointment Background Investigation Requirements for Appointment to Critical-Sensitive Positions

This is a request for a waiver of the pre-appointment background investigation requirements for James Sullivan III's appointment to a critical-sensitive position. This individual has been selected for the position of Senior Advisor with the Office of the Director.

Executive Order 10450, "Security Requirements for Government Employment", Executive Order 12968, "Access to Classified Information", and Security Executive Agent Directive 8, (SEAD 8) provide that in exceptional circumstances or in an emergency, when official functions must be performed prior to the completion of the investigation and adjudication process or when in the national interest, an individual may be appointed on a temporary basis to a critical-sensitive position prior to the investigation's completion. A delay in appointment would be harmful to national security and adversely impact the organization's mission.

Upon approval, the U.S. Office of Personnel Management's (OPM's) Personnel Security will initiate the above-named individual's personal security package for an expedited background investigation and pre-waiver checks, as appropriate. It is in the Agency's best interest to affect this appointment as soon as possible.

(Note: A waiver cannot be issued unless mandated portions of the current Tier 5 have been favorably reviewed.)

DECISION:
☒Approved ☐Not Approved ☐Let's Discuss

Recoverable Signature

X Jennifer Duncan

Branch Chief, OPM-FSEM-Personnel Security

Signed by: Office of Personnel Management

U.S. Office of Personnel Management

This is to certify that

James Sullivan

has completed the course

CY 2024 Classified National Security Information Awareness and Insider Threat Training

March 8, 2025

Tierra F. Elsey