ICIT | Institute for Critical Infrastructure Technology

Preparing the Battlefield: The Coming Espionage Culture Post OPM Breach

Institute for Critical Infrastructure Technology

August 2015

Imagine what you could do with a database of detailed and accurate, biographical and personal information of every denizen of the seven largest cities in the United States: New York City, Los Angeles, Chicago, Houston, Philadelphia, Phoenix, and San Antonio. Now, imagine the possibilities if those cities were filled to capacity with every member of the intelligence community and you knew everything about them, including their strengths, their weaknesses, and their vulnerabilities. Right now, somewhere across the globe, an unknown actor group has the information of the 15% of the American population who have applied for a security clearance since the year 2000.The information likely has not been used yet or sold on darknet markets; but, there is no doubt that whoever holds the data is considering the possibilities.

Background:

In June 2015, the United States Office of Personnel Management (OPM) disclosed an October 2014 breach of systems maintained at a Department of the Interior shared-services data center which lead to the exposure of an estimated 4.2 million personal records. About a week later, investigators from U.S. CERT and DHS discovered and disclosed a larger breach of the OPM systems dating to March 2014. Applicants for clearances complete a 127 page Standard Form-86 (SF-86) which contains all of their personal information, work history, family, associates, deviances, and proclivities. In the latter breach, an unknown adversary compromised the antiquated network of the United States Office of Personnel Management and obtained these SF-86 forms. Consequently, an unknown adversary now possesses the granular personal information belonging to the 19.7 million United States citizens who have requested or possessed a security clearance since the year 2000. Even worse, the amount and

detail of information about each victim increases in proportion to the individual's level of security clearance. This means that individuals with the highest clearance levels are at the greatest risk of exploitation.

The length of the breach and the sophistication of the malware used to compromise the OPM network presents evidence of a persistent targeted attack. While targeted attacks aren't necessarily more advanced than others, except in the sense that a high-value target might require a greater degree of sophistication, though this was not the case with OPM. Persistence is a characteristic of targeted attacks because they persist in the face of the victim's security controls instead of moving on to weaker targets. Similar to Advanced Persistent Threat (APT) groups, perpetrators of these targeted attacks are motivated and highly dedicated adversaries who often receive resources and direction from larger organizations, such as nation states. While APT activity can be identified through discernable operational patterns, remaining indicators of compromise of target systems, target profiles, coordination of attacks, resource investment, and the sophistication of the attack targeted can prove to be more difficult. Traditional network and host-based intrusion detection and prevention techniques are useful but are many times insufficient. The Ponemon Institute reported in their State of Advanced Persistent Threat report that 72% of survey respondents indicate that exploits have evaded their IDS and 76% say malware has evaded their A/V solutions. Trend Micro reported that 55% are not even aware of intrusions and fewer know the extent of the attack or who exactly is behind it. Whether part of a targeted attack or APT activity, attackers operate as an invasion force. They tenaciously pursue their goals by utilizing a wide range of tools and tactics that best allow them to steal data, destroy infrastructure, or poison trusted stores of information

undetected. They often acquire specialized information about the target, its infrastructure, and its personnel prior to a dedicated attack. The information is used to initially compromise the target, establish a foothold in their systems, and strengthen the adversary posture by establishing backdoors and laterally moving to compromise other systems. The adversary uses prolonged internal reconnaissance to identify valuable data, the adversary exfiltrates data over an extended period, and then the adversary moves laterally to another system to repeat the process until all valuable information is harvested or the breach is detected. Sometimes the malware or tools in the attack are specialized and can be used to attribute the attack to an actor group. Other times, information about the target and data stolen can be used to guess the motivation of the attack and narrow attribution to a pool of possible actor groups. However, adversarial motivation is difficult to portend because organizations do not always recognize the value of their data or consider that their adversaries may have targeted an organization in order to gain access to a different organization.

Details confirming how adversaries breached OPM and the indicators of compromise necessary for accurate attribution of the attack remain classified. Cyber attackers are either organized criminals, state sponsored hackers, or a hacktivist group. Criminal attackers seek economic gain whereas state sponsored actors mount attacks to steal intellectual property, gain economic or political advantage, or support intelligence or counterintelligence efforts, and hacktivist groups seek to acquire information to expose and/or embarrass the target of their attacks to achieve a political or personal result. Numerous officials, including U.S. Intelligence Chief James Clapper, have attributed the attack to China. FireEye, iSight Partners, and other firms attribute the attack to a Chinese state sponsored APT group referred to as “Deep Panda”

by Crowdstrike or Black Vine by Symantec. Deep Panda steals PII from U.S. commercial and government networks for Chinese intelligence and counter-intelligence purposes. The group uses social engineering, phishing schemes, or 0-day exploits to gain access to a network, establish a persistent presence, and deploy remote access Trojans (RATs) that allow recording and seizure of user sessions. Tools such as Scanline and PwDump are used to acquire legitimate credentials that the actors can utilize to escalate their privileges, create unmonitored accounts, or move laterally to other systems. The recent Anthem, VAE, Premera, Empire Blue Cross Blue Shield, and Carefirst breaches are attributed to Deep Panda.

The PII, work history, and organizational information compromised in the Deep Panda breaches mentioned are categorically identical to the information targeted in the OPM breach. The group has employed RAT's from the Sakula malware family in past incidents. Post OPM release of FBI-000061, warning agencies of the Sakula malware has fueled online speculation of its use, and Deep Panda's involvement, in the OPM breach. Further, in Threat Connect's analysis of the VAE and Anthem breaches, malicious domains targeting OPM (www[.]opm-learning[.]org and www[.]opmsecurity[.]org) were discovered to be linked to known command and control (C2) servers, which act as an adversary's "dropbox" or hop point for exfiltrated data. APT's often use phishing sites such as these to trick users into revealing legitimate credentials or to make spear phishing emails seem legitimate. These two domains were registered with 10 character random alphanumeric [.]gmx.com email addresses and Avenger (Steve Roger, Tony Stark, etc.) registrant names to a GoDaddy name server. Moreover, the opmsecurity domain was registered on April 25, 2014, 4 days before the registration of the theWe11point[.]com domain used in the Anthem breach and a few weeks prior to the first

OPM breach in March 2014. The domain, opmsecurity, remained dormant until December 18, 2014, which may coincide with the December 2014 second OPM breach. OPM publically announced awareness of the second breach on June 4, 2015 and as a matter of coincidence or intent, the last observed activity on the opmsecurity domain was June 3, 2015. Further, unconfirmed online reports assert that the certificate assigned to the malware used in the OPM breach was signed by DTOPTOOLZ, a stolen certificate used in the Anthem breach. Threat Connect asserts with high confidence that this evidence indicates that the actor behind the VAE and Anthem breach is also the actor behind the OPM breach.

The actions of those responsible for launching the attacks on OPM can be best categorized as "Preparing the Battlefield". Given the long term unprotected state of OPM's systems at the time of the breach and its susceptibility to attack, it is possible (and likely) that the OPM breaches were simply successful expeditionary attacks against the United States Government. OPM is not the first and will not be the last agency to be targeted by foreign entities seeking to do harm to the United States. The most likely scenario is that even now there are hackers inside the systems of other agencies who have been there for some time. Vandals and criminals go after quick payoffs and easy returns, but foreign governments can have unlimited patience. Once a system has been penetrated those who did it may sit on it and observe until they feel the time is right. They may even patch vulnerabilities behind them so no one else attempts to breach the system and set off alerts.

Worse, United Airlines recently disclosed a breach of its system and the attack has been attributed to Deep Panda due to a malicious domain registered to Marvel comics character

James Rhodes. Investigators do not yet know the scope of the breach, the amount of data stolen, or the timeframe of that data. It is believed that the adversary exfiltrated flight manifests containing passenger information (name, birthdate, etc.), and origin/ destination information. Since United Airlines is the second largest airline in the United States, the actor could possess considerable data even if the scope of the breach was limited. American Airlines has also recently disclosed details of a breach of its systems and it is believed to be the same bad actor that perpetrated the United Airlines breach. This means that a single, potentially state sponsored adversary possesses the granular information of practically the entire United States intelligence community, their health records, and their travel plans. If the actor group is criminal, then victims only have to worry about financial impact, which can be mitigated through vigilance, credit freezes, and the credit monitoring service that is offered by the Federal government. If the actor is state sponsored, then the global cyber-battlefield has just been drastically and permanently altered. A state sponsored actor may use the trove of information to construct a database reminiscent of LinkedIn or Facebook for their intelligence community. Given the pool of information, the combination of the stolen databases could devastate the United States Intelligence community for at least the next 30 years.

Hot Topic in a Cold War:

Breaches are like waves in the ocean. They constantly batter at our shores until the water level slowly overtakes the country. The OPM breach was not even the first significant breach this year, and it will not be the last significant breach in our lifetime; yet the OPM breach was a very large wave. It is unique in that it affects the entire nation and that the lost

data has the potential to exponentially increase the rate and success of breaches against other facets of the federal government. The United States government must reform the technological foundation and the practices of its cybersecurity posture before the next wave hits.

Every day, private businesses and government agencies are engaged on the multiple fronts of the cyber battlefield. The war is fought with information and disinformation instead of bullets and missiles. The unknown cyber-adversaries are apparitions in the wilderness of mirrors. More than two decades of terrible cybersecurity practices and disinterest in cyber-infrastructure investment has left the United States unprepared for this war. Federal agencies lack the skilled personnel, the resources, and the technology necessary for success. Without immediate reform, the United States will not be able to stave off its adversaries.

The adversary can employ big data systems which can be used to predict the behavioral patterns of American Intelligence officials. Development of such an application is likely why the information has not been used yet. Moreover, combined with the information stolen from United Airlines, the actor can track the travel patterns of officials, military personnel, and contractors. The foreign associates and relatives declared on victims' SF-86 forms are already at risk of exploitation or worse. Big data analytics can be used to correlate the travel information with the base / station of OPM victims and with knowledge of a known or suspected foreign contact be used to expose United States confidential dealings with foreign assets. Within a few hours, the state sponsor could use this information to eliminate every counterintelligence asset residing in their country. United States intelligence operatives, who did not complete OPM paperwork, may now be at considerable risk as well.

The remainder of the victims may be subject to economic exploitation, blackmail, threats, coercion, public embarrassment, and many other possible tragedies. Agencies can help themselves and employees by discussing these possibilities in open forums. Malicious actors currently possess the personal information of federal employees. While some would be angered and distrustful of the federal government by this alone, the malicious actors also have information about those employees' families. No matter what compromising information about an individual was in the SF-86 forms, the information about their family will be more influential in extortion attempts. The least agencies can do when federal budget constraints and mismanagement lead to malicious actors knowing the address where the children of federal employees attend school, is create an understanding and open environment where concerns can be freely discussed without fear of loss of reputation or consequence. Further, instituting policies incentivizing employees to report exploitation attempts, without consequence, will greatly decrease the likelihood of insider threat attempts. Even if employees remain honest, they are less likely to report blackmail or counter-intelligence recruitment attempts if they fear for that doing so will result in loss of their career or status. Employees know what is in their forms. They need to do two things. First, they need to request a copy of their SF-86 and validate that their information is correct. Then they need to ensure that nothing in that form can harm their personnel lives. This means enacting credit freezes and monitoring accounts on a weekly basis, because credit monitoring does not actively prevent identity theft. Employees also must change passwords to robust strings that do not pertain to their personnel life and change security questions to not actually correspond to the victim. Antivirus and firewall software on personal computers should be configured to strict settings. Details about the victim and big

data behavioral profiling is going to make spear phishing campaigns, where a specific individual is targeted by a scam email containing malware, more prevalent. Emails should only be opened if they are confirmed to be from a safe contact and not a phishing scheme that is imitating a legitimate contact by using a typo in their name. Email attachments should be scanned before opening and email links should never be followed. Employees need to lock down the privacy controls on their professional and social accounts. These daunting efforts may cause some employees to withdraw from the internet. Agencies need to warn against this behavior for the sake of the professional community. The government is going to have a very difficult time recruiting skilled employees in the next few years and it must help its current employees to flourish. Employers research candidates online. One of the largest red flags against a potential new hire is lack of an online presence for those under the age of 50. If victims withdraw from online activities, their careers will stagnate or solely remain in the federal government. Connections to the private sector will diminish and the nation will suffer.

Agencies need to reform their cybersecurity practices and posture in novel ways. The nation need to get over the "Woe is me, how could this have happened" mentality. After the past two years have shown us that no organization is immune to cyber-attack, the United States needs to stop hitting the snooze button on cyber-reform. On July 15, 2015, at House Oversight hearing on Cybersecurity at The Department of the Interior, Representative Will Hurd (R-TX) remarked, "It is no secret that Federal agencies have a long way to go to improve their cybersecurity posture. We have years and years of reports highlighting the actions and vulnerabilities of Federal agencies. We also have years and years of recommendations from IGs, GAO, and experts in and out of the Government on how to address these vulnerabilities. Simply

put, we know what needs to be done; we just need to do it." Federal agencies face budget constraints, lack of skilled personnel, and lack of resources. However, it is difficult enough for large private companies with plentiful resources like JP Morgan-Chase, Anthem, United Airlines, and Target to defend against the sophisticated attacks that result in the loss of personal identity and financial information of millions of their customers. OPM's assistant to the inspector general for audits, Michael Esser adds, "Resources, I think, are always an issue, but are not the sole answer. Sometimes [the OIG] feel things we report don't get the attention that they deserve." Agencies need to slow new initiatives and focus on meeting the basic requirements and recommendations in the inspector general reports. Both private and public organizations need to change their approach and execution of cyber security best practices rather than trying to pay for the problem to go away.

OPM failed because it lacked a fully implemented governance structure, it failed to properly assess system vulnerabilities, and it did not use robust authorization mechanisms. Many agencies still have inconsistent implementations of agreed upon governance frameworks for information security and ineffective system assessment and authorization mechanisms. OPM's lack of a cohesive vision and direction on how to best protect its systems/data, including the types of resources, skillsets, and tools needed, demonstrated that well-meaning personnel when tasked with IT tasks outside their regular professional core competencies are just as dangerous as malicious insider threats. Agencies need to employ trained IT staff to maintain systems and trained cybersecurity staff to work with IT and maintain information security protocols.

The information from the OPM breach and the publication of how easy federal legacy systems are to compromise will result in cascading breaches at other agencies. Agencies must treat every system as compromised and shore up their defenses until they can guarantee otherwise. They can reduce their attractiveness to attackers by collecting less information and by imposing data retention limits. They can also increase security by properly vetting contractors and by not engaging in "lowest bidder" contracting.

Current efforts and the media have focused on the identity theft and loss of personal information as the biggest issue to come from these breaches when espionage is the largest looming issue that has not been directly addressed, but should be. In its current state no one can vouch for the integrity of ANY of the data in the OPM database. There are already protections in place in the financial industry to protect the credit and financial well-being of those whose data was taken. To continue focusing on identity theft clouds the landscape of potential disasters that may be looming and siphons off already taxed resources from chasing down problems of greater severity. Creating and inserting false records into the OPM database or tampering with/editing existing records would be basic data entry for someone with the level of credentials that were in use by the bad actors who planned and executed this hack. What good would these actions do for those who spend the energy to achieve them? Distilling this down to its most basic application the clearance information dictates level of access, both physical and logical, to United States Government facilities and systems around the world. Think about the possibilities if those who seek to do harm to the United States and its citizens, and allies suddenly have unprecedented access to facilities that they did not have before. Doors could literally be opened for physical attacks as well as further penetrations of critical

infrastructure systems. Why would enemies of the United Stated spend time and resources developing new avenues of attacking systems and attempting to circumvent system security controls when they could simply raise the system and/or building access of someone who could just walk in the door and log in to a system whose data they desired to acquire or corrupt?

Outside the increased threat of physical attack due to elevated system and physical access there exists an even larger and longer term threat. The data lost by OPM contained not only the information of former, current, and potential employees it also contained detailed information about their families, employers (past and present), friends/colleagues, and travel habits. The threat posed by the sheer depth and complexity of this data is its value as fuel for social engineering to expand the attack footprint of the initial breach. We cannot assume that only those whose data was compromised are at risk. Everyone and every organization a victim detailed involvement with is at risk of being targeted. Here is where things are even worse than are being represented by OPM and OIG. The SF-86 forms that were stolen are the holy grail of Counter Intelligence operations against the United States. In addition to the data concerning prior employment details and personal/professional relationships they also contain detailed accounts of the applicant's personal weaknesses, drug problems, family problems, legal issues, and more. By all accounts the Chinese and other foreign governments are, in layman's terms, building their own massive databases on US Federal employees for the purposes of building a robust system for offensive counter intelligence. Think of is as the Facebook or LinkedIn of counter intelligence targets in the U.S. Government. The reasoning for why anyone would do that is simple: offensive counter intelligence[6]. While defensive counterintelligence, the preventing and uncovering of enemy spies, is the basic level of counterespionage programs the

most critical damage they can bring to bear is in offensive counterintelligence. This targets the recruiting of spies inside an enemy organization, in this case the United States Government. It would be considered a major coup for any CI (Counter Intelligence) organization to recruit operatives inside the opposing intelligence service of an enemy state. Understanding what your enemy knows about you in this manner is the easiest way to craft a plan of deception at the tactical and strategic level. The playing field is no longer even based on the information that was accessed in the OPM systems. It is no coincidence that the databases targeted in the hack contain the deeply personal information of the keepers of America's secrets including uniformed intelligence officers and counter intelligence officers. Any hostile organization possessing this data will be able to perfectly select targets for recruitment, intimidation, blackmail, and coercion with attacks tailored using the intimate personal details (good and bad) of their lives. Additionally there is an unstated threat posed to the children of those affected by the breaches of the OPM databases. What was once in the realm of fiction writing is now fully within the realm of possibility in the cyber age. Targeting children of Federal employees for early recruitment, blackmail, or other nefarious aims is now a much simpler and tantalizing prospect for any hostile entity just based on the sheer volume of highly detailed information that was accessed in these breaches. The ability to utilize detailed family histories, personal medical/health information, education records, and the like gives anyone interested in developing the friends and family members of US Federal employees (and contractors) into intelligence assets a huge advantage in the game. There are no targets that will be considered "out of bounds" in these efforts. In some cases we are already dealing with opponents who routinely and forcibly conscript the children of their own citizens into sports/athletic programs

to further their own national image and glory. If they are willing to kidnap and institutionalize the children of their own citizens is it reasonable to think that they would show any compassion or consideration for the children and families of their perceived enemies? The answer is a resounding “No”. In addition to targeting U.S. Nationals any foreign entity now has a detailed listing of their own citizens who may have “close and continuing contact”, to cite security clearance lingo, with American Government officials. It does not require imagination to understand how another foreign government would seek to exploit those ties for the purposes of espionage against the United States. While U.S. agencies are scrambling to plug the leaks and bring systems up to par with information security best practices a massive blow has been dealt to U.S. Intelligence and Counter Intelligence that will be felt for decades to come and may not be recoverable.

Every public and private company that employs cleared employees is at risk of insider threat from blackmail, or altered data in the OPM databases. The data in these systems needs to be validated or the entire clearance system needs to be scrapped. If OPM had air-gap or change managed redundancy servers, then checking the data is as easy as cross checking the two systems and investigating the discrepancies and all accounts created after the initial breach. Since OPM probably did not have comprehensive backup systems, alternatives must be considered. Every clearance could be reissued to known employees. This solution is costly, time consuming, and it demands that the actual clearance of every victim is accurately known. There are a number of possibilities of varying scope and complexity to mitigate these risks. Regardless of next steps undertaken to verify the veracity of the data and the clearances it provides any

future plan for the OPM systems, and others, must provide for this capability moving forward or this is a continuing self-imposed threat.

Combined the attacks against JP Morgan, Target, Home Depot, and others will not have as significant an impact on national security as the OPM breach. The combination of data types that was culled from the OPM databases presents a clear threat to the national security of the United States and a direct personal threat to those citizens whose data was affected. Agencies need to take strides to protect themselves and their effected employees. Training in cyber-security best practices will help repel two decades of appalling practices. Names and personal details need to be disassociated from federal login and email accounts. An identification string consisting of letters and numbers is more difficult for an adversary to guess and compromise the network. The strings should periodically retired (every 6 months or so) and new strings should be issued. This minimizes the impact and lifetime of leaked credentials. Employees can either memorize the login information or agencies can issue badge cards with the login, but not the password. Though not the best practice, providing employees with random string logins that they have to write down, are still more secure than accounts corresponding to employee names, badge number, or personal details.

Biometrics: An Eye to the Future

Access can be granted to an individual based on what you know (a password) what you have (a token) and who you are (a biometric indicator). Tokenization and biometric systems are initially expensive but, agencies should weigh the investment against that of another breach when

making a decision. A token is a physical device, such as an encrypted RFID chip, that grants access to the person who has it. These can be key fobs or wrist bands. Hackers cannot breach the system without stealing the token and then inputting the second factor (usually a password). Multifactor identification is needed to mitigate the impact of the OPM breach, but is just one small piece in what needs to be a larger and more holistic strategy of Identity, Credential, and Access Management (ICAM) for Federal employees and contractors interacting with Government systems and data. Simply implementing multi-factor authentication without the careful consideration and inclusion of management strategies for establishing and monitoring Digital Identity, Credentialing, Privilege Management, Authentication, Authorization & Access, Cryptography, and Auditing & Reporting would be a half measure.

Biometric indicators are measures of what makes a person unique, such as fingerprint or retinal scan. Agencies can implement fingerprint scanners or other biometric devices to improve security. Some devices, such as keystroke dynamics are un-invasive. Keystroke dynamic systems measure the time a person depresses keys and the time between different keystrokes to build a profile that identifies who is at the keyboard. Voice identification and retinal scan systems are also improving in accuracy. Biometrics is an effective way to prove the identity of an individual with a great level of assurance. Accountability is ensured because the person accessing an area or resource has to be the person possessing the biometric.

In addition to the 22+ million records that were breached it has been discussed that there were also at least 1.1 million sets of fingerprints belonging to United States Government employees accessed in the latest breach of OPM systems. “It's probably the biggest counterintelligence threat in my lifetime," said Jim Penrose, former chief of the Operational

Discovery Center at the National Security Agency and now an executive vice president at the cybersecurity company Darktrace. "There's no situation we've had like this before, the compromise of our fingerprints. And it doesn't have any easy remedy or fix in the world of intelligence." It is also speculated that the bulk of the biometric data accessed were digital scans of fingerprints and not the older form of printed fingerprint cards. This would mean that these fingerprints belong to current and recent government employees. In order to enhance security in recent years systems have begun relying on multi-factor authentication which many times can include the use of finger prints. Fingerprint scanners work by saving an approximation of your fingerprint and comparing it against your finger on the scanner. As recently reported by Andrea Peterson in the Washington Post, skilled hackers could breach a system to acquire and utilize a scan of an individual's fingerprints to gain access to an area or digital resource. Unlike social security numbers, addresses, and passwords fingerprints cannot be changed or reissued. Once in the hands of bad actors they are a threat for as long as the service life of the person they belong to. If access controls management is not closely monitored by an agency it could be even longer. As of mid-July it is still unclear whose fingerprints were included in the 1.1+ million fingerprints affected. While the CIA might be in the clear, because they maintain their own records outside of OPM, nearly every other agency is affected. This includes the employees of the Federal Bureau of Investigation, National Security Agency, and anything housed under the umbrella of the Department of Defense[8]. As biometrics becomes a more critical part of major security schemes the value of the data affected increases exponentially. U.S. agencies will need to re-assess the authentication methods in use or under consideration, especially if they are dependent on fingerprints. There

are a number of nightmare scenarios that play out when considering the implications of stolen biometrics data along with the detailed personal history of U.S. Government personnel. One solution that could be a game changer is a new biometrics-based authentication methodology being researched by the Defense Advanced Research Projects Agency (DARPA). The Active Authentication program DARPA has initiated is developing new ways of validating the identity of a user through the use of software based biometrics, one or more intrinsic physical or behavioral traits that can be associated with a specific individual

As the reliance on biometrics to confirm our identities has grown here in the U.S. so too has it around the world. What are the odds that an undercover operative traveling across international borders under an assumed identity may be captured by a foreign government using fingerprint scanning as a biometric identity confirmation tool? Possibilities like this are no longer in the realm of Hollywood fiction. These threats are real, advanced, and persistent; and currently there is no way of correcting them shy of simply removing assets from the field. Consider the damage of having a significant portion of U.S. Intelligence and Counter Intelligence sidelined in this fight. Without even knowing who was contained in the biometrics data breach the United States has no idea just how bad the initial attack has been and who may be in immediate danger as a result.

The OPM breach is only the first of many major breaches in an oncoming storm of cyber-warfare against the United States. So, anticipating more of the same we must have better Incident Response plans and response teams prepared and waiting to act. Notification services and methods must also be prepared in advance to provide rapid and accurate notice to those

affected in future incidents instead of taking months as it has (and is still ongoing) with OPM. To reduce the number of potential breaches from insider threats, the federal government must be ready and it must do what it can to limit the effects of the information stolen from OPM and it must eliminate any information added or altered in the OPM database. The federal government can use its people to validate the information in OPM's system and root out any bad actors. Afterward, critical cyber-infrastructure can be improved, the identities of American citizens can be protected, and this nation can gain control of the battlefield.

*Expert research contributed by the following ICIT Fellows:

- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Drew Spaniel (ICIT Visiting Scholar, Carnegie Mellon University)
- Chris Schumacher (ICIT Researcher)
- Stan Wisseman (ICIT Fellow, Security Strategist, HP)

Contact Information

Legislative Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies, Executive Branch and Fellow Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

Social Media:

AFCEA

http://www.afcea.org/content/?q=Article-disruptive-design-death-password

ARS Technica

http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/

The Baltimore Sun

http://www.baltimoresun.com/news/maryland/bs-md-federal-workplace-opm-20150721-story.html

Bloomberg

http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines

CIO

http://www.cio.com/article/2947453/data-breach/how-opm-data-breach-could-have-been-prevented.html

CSO Online

http://www.csoonline.com/article/2852855/advanced-persistent-threats/10-deadliest-differences-of-state-sponsored-attacks.html

Fed Scoop

http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community

Federal News Radio

http://federalnewsradio.com/opm-cyber-breach/2015/07/federal-news-radio-opm-hack-survey-07-22-2015/slide/1/

http://federalnewsradio.com/fed-access/2015/07/the-opm-cyber-breach-and-the-cleared-community/

Federal Times

http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/07/10/lifetime-credit-monitoring-opm-breach/29958383/

FireEye

https://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf

Fox News

http://www.foxnews.com/tech/2015/07/14/why-opm-hack-is-ongoing-cyber-headache/

Huffington Post

http://www.huffingtonpost.com/adam-levin/open-letter-on-the-opm-br_b_7766708.html

[id] Management (a US Governement website)

http://www.idmanagement.gov/identity-credential-access-management

Info-Security Magazine

http://www.infosecurity-magazine.com/news/us-house-intros-lifetime-credit/

Military Times

http://www.militarytimes.com/story/military/capitol-hill/2015/07/13/hasc-opm-data-breach/30080025/

National Journal

http://www.nationaljournal.com/tech/opm-hack-fingerprints-china-20150714

Office of Personnel Management

https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/

PC World

http://www.pcworld.com/article/2954872/opm-anthem-hackers-reportedly-also-breached-united-airlines.html

Tech Zone 360

http://www.techzone360.com/topics/techzone/articles/2015/07/10/406516-what-need-know-the-opm-data-breach-incidents.htm

Washington Technology

https://washingtontechnology.com/articles/2015/07/31/agg-opm-breach-cyber.aspx

Wired Magazine

http://www.wired.com/2015/07/senator-sasse-washington-still-isnt-taking-opm-breach-seriously/

The XX Committee

http://20committee.com/2015/06/08/hacking-as-offensive-counterintelligence/

http://20committee.com/2015/06/11/the-opm-hacking-scandal-just-got-worse/

Youtube

https://www.youtube.com/watch?v=5Hzcq_ap0ck