CMS
ISSO Journal

...by and for CMS Cybersecurity Professionals

April - June 2022
Issue 20
The CMS ISSO Journal seeks to help enhance the proficiency and capabilities of the CMS Cybersecurity Community.

Published Quarterly, the Journal shares professional experiences and expertise of the CMS ISSO community, cybersecurity contractors, and interested CMS professionals.

The CMS ISSO Journal is freely distributable without restriction within and outside of CMS. You can find the ISSO Journal in multiple locations, including in Confluence at “ISPG ISSO Workforce Resilience Program” and in CFACTS. If you need a copy, send a request to isso@cms.hhs.gov

Articles published in the CMS ISSO Journal are eligible for continuing education units. If you have something that you want to share, let us know by sending an email to isso@cms.hhs.gov.

How are we doing? Let us know by sharing your thoughts on this or other issues in a brief survey at https://cmsgov.typeform.com/to/vPFO8LfU

The CMS ISSO Journal is freely distributable without restriction within and outside of CMS. You can find the ISSO Journal in multiple locations, including in Confluence at “ISPG ISSO Workforce Resilience Program” and in CFACTS. If you need a copy, send a request to isso@cms.hhs.gov.
**Welcome to the 20th issue of the CMS ISSO Journal**

It is hard to believe that it has been four years since the CMS ISSO Journal began, and that this is the 20th issue. What started out as a monthly publication pilot project to get ISSOs talking has gone through bumps and starts. It is a challenge to find content, and yet ISSOs and others still feel that the Journal provides value based on a recent TypeForm survey.

In recognition of this milestone, this issue will be a bit different. We have gone through some of the past issues and are re-presenting some articles that a) have aged well and b) represent particularly outstanding value to ISSOs. These “From the Vault” articles will accompany our normal updates and information. This issue’s articles include an early 2019 piece by Jamal Webster of CGI on CDM. We also include an interesting primer on 5G by Eric Brockman and Omiome Olaghere, Assyst Services CRAs. We look to continue this practice in future issues.

New work in this issue includes work from contributors Chris Hughes, John Hoeg, John Laycock, Elizabeth Schweinsberg, Lawrence (Larry) Grim and Eric Larson. There is informative information on DevSecOps and Zero Trust, as well as analysis of the Okta compromise and a lesson learned with privately-procurred resources.
Journal Contents

The 7 Most Common Ways to Fail with DevSecOps .......................................................... 4
Malware Risks with PIV and CAC Card Readers ............................................................. 8
LAPSUS$ Group .............................................................................................................. 9
CMS Zero Trust Maturity Framework is coming! ............................................................... 11
From the Vault: Continuous Diagnostic Monitoring (Jan-Feb 2019 Issue) ......................... 12
From the Vault: The 5th Generation (5G) Networking Evolution (June July 2020 Issue) .... 13
ISSO Open Mic .............................................................................................................. 16
Are You a New ISSO, Or Do You Know One? ................................................................. 17
What’s HOT? .................................................................................................................. 18
Gaining Access to HHS Resources ............................................................................... 19
Cybersecurity Community Forum Notes for April and May 2022 .................................... 22
Data Guardian Update ................................................................................................... 23
Adjusting Meeting Frequency ......................................................................................... 23
Combatting Insider Threats within CMS ....................................................................... 23
Understanding the Risks of Federal Foreign Travel ..................................................... 24
Phishing Results February 16 – 19 ............................................................................... 24
CMS Information Security Advisory Board (CISAB) Update ........................................ 25
Training Update ............................................................................................................ 26
Getting Your Role-Based Training Requirement Completed ........................................ 26
New Two-for-One Training Deal! .................................................................................. 26
Internal and External Resources for ISSOs ................................................................. 26
The 7 Most Common Ways to Fail with DevSecOps

Chris Hughes, Aquia, Inc.

Editors Note: In this article the author discusses information related to DevSecOps in general. In upcoming issues he will apply this directly toward ISSOs.

Organizations are increasingly striving to adopt DevSecOps. This is being done for a variety of reasons, from the increased digitization of society, market pressures to deliver value faster, seeking to maintain competitive advantages, looking to decrease the cost of security remediations and more. However, despite the rush to adoption, there are several ways organizations are failing with their adoption efforts, we will discuss some of them below.

Failing to Establish a Learning Culture

Organizations are increasingly striving to adopt DevSecOps, but in doing so, they must embrace a culture of continuous learning and experimentation. In the seminal work “The DevOps Handbook”, it is emphasized that to be successful with DevSecOps and building on the success of high-performing organizations, a learning culture is key.

This is facilitated through daily learning, reserving time for organizational learning and improvement and a concentrated investment by the organization in upskilling the workforce. This materializes itself in various forms, such as learning subscriptions, tuition assistance, certification reimbursement and brown bag sessions, where subject matter experts both from inside and outside the organization can share expertise and lessons learned.

The impact of talent and cultural issues cannot be emphasized enough. In a recent report from McKinsey, it was identified that talent and cultural issues pose the greatest challenge to technology transformations, which includes DevSecOps.

Neglecting Cross-Functional Education

Building on the need for learning, as part of a broader imperative to break down silos, cross-functional education must be pursued. There is an often unspoken but widely recognized tension between the Development and Security teams.

In the 2020 FOSS Contributor Survey conducted by The Linux Foundation and Harvard’s Laboratory for Innovation Science, it was found that the average FOSS developer only spends 2.3% of their time improving the security of their code and they utilized terms such as “soul-withering” to describe secure coding and security. In a time where organizations are looking to “shift security-left”, developers are in a prime position to mitigate security vulnerabilities before commits and production promotion and they must understand the organizational value of secure coding and be incentivized to pursue it.

On the flip side, we are finding ourselves in environments where everything is increasingly becoming code. From application code, Infrastructure-as-Code (IaC)/Compliance-as-Code, Kubernetes manifests and CI/CD pipeline YAML templates, code is everywhere. Security professionals do not necessarily need to be excellent developers, but they should certainly make an effort to understand the coding practices at a high level and be
able to review templates for common misconfigurations and vulnerabilities. This would also improve collaboration and common ground between the two groups.

**Neglecting to Communicate Business Value**

Any endeavor pursued by an organization, including DevSecOps, should be tied to key business objectives and goals. DevSecOps is a transformational journey that requires buy-in and engagement from critical stakeholders across the organization.

For this reason, it is critical to communicate the business value of its pursuit. Senior leadership must clearly understand the “why” of pursuing DevSecOps. One of the most effective ways to do this is through metrics. Many are familiar with the popular DevOps Research and Assessment (DORA) metrics from the popular book *Accelerate,* but that is just a start. Organizations can, and should, utilize additional metrics as well. As Bill Nichols from the Carnegie Mellon Software Engineering Institute (SEI) states, “measurements must be accessible, available and related to business goals.”

Communicating the business value of DevSecOps adoption and utilizing metrics to support it can go a long way in securing support from key stakeholders and executive leadership within your organization.

**Being Too Risk Averse, Fearing Failure**

As previously mentioned, high-performing organizations and teams successfully adopting DevSecOps embrace a culture of learning. The antithesis of this is being too risk adverse and fearing failure. Failure is a natural byproduct of the learning process.

If your teams and staff are not in a position where they can make mistakes, obtain lessons learned and iterate on those failures, the chances of successfully adopting DevSecOps is increasingly slim. Teams must be empowered to learn, identify their weaknesses, build on them and improve in competencies. This only happens in an environment built on transparency, safety, and trust.

Another key component of being overly risk averse is allowing security to be primary point of friction and contention among DevSecOps implementations. A common complaint about security in environments implementing DevSecOps is that it is simply too cumbersome and just slows down innovation and delivery. This complaint is not entirely without merit. Organizations must find ways to implement security as frictionlessly as possible. This is seen by integrating with developer workflows, embedding security subject matter experts with development teams, establishing security champions among development and as discussed below, embracing a culture of security across the organization.

**Tool Sprawl and Fragmentation**

With the increased pace of digital transformation and innovation, we are seeing a rapid growth among the cloud-native landscape. That growth provides a vast and rich selection of tools and applications to help facilitate organizations DevSecOps goals. However, that rapid proliferation of tooling also provides an increasingly complex and disjointed environment for many organizations. One must look no further than the most recent Cloud Native Computing Foundation (CNCF) landscape to just an idea of how diverse this landscape has become.
Organizations are increasingly running into challenges around visibility and productivity due to toolchain sprawl. They are also seeking to embrace toolchain management options in attempts to get a handle on the sprawl and the associated inefficiencies it is causing.

These issues are not just isolated to Development and Operations either. Security is also encountering its own challenges associated with tool sprawl. In the 2020 Cloud Security Alliance (CSA) “Cloud-Based Intelligent Ecosystems” findings show that most organizations are struggling with identifying how well their security tooling is working if it is generating value ROI and that their teams are struggling to even keep up with the tools in their environments.

In a rapidly dynamic and evolving IT ecosystem like we find ourselves in, tool sprawl and fragmentation are real threats. They impact visibility, productivity and most importantly, security. Threats continue to proliferate and if your organizations lack real visibility and control, you are certainly at risk and you do not even know it.

Security Culture

Organizations and the industry simply do not have enough security professionals. In the ISC2 2020 Cybersecurity Workforce study, it was identified that there is a global shortage of 3.12 million cybersecurity professionals.

Security professionals are outnumbered at organizations compared to their development and operations counterparts. Couple that with the reality that developers are in a key position to mitigate security concerns earlier in the Software Development Lifecycle (SDLC) and operations teams are primed to identify operational anomalies and it must be a team effort.

Establishing a security culture starts with the realization that security is the responsibility of everyone involved. Communication and awareness of some of the primary security concerns and principles can also go a long way. Security teams and staff must shift from being seen as the office of “no” and instead viewed as a collaborative partner that can help achieve shared outcomes, while integrating key security requirements throughout those endeavors.
Thinking You Can “Buy” DevSecOps

Many organizations mistakenly begin their pursuit of DevSecOps through the lens that you can simply “buy” DevSecOps. For example, if we implement CI/CD pipelines, we are doing DevSecOps. This is simply not true.

DevSecOps is a methodology, one that is facilitated through people, processes, and technology, with the first two potentially being even more important than the last. Without making the effort to implement a culture aligned with agile and DevSecOps principles, it is unlikely you will find a successful DevSecOps implementation or maturity.

The same can be said for failing to update and implement new organizational processes aligned with said principles and practices. Forcing old operating models into modern technologies and practices simply lead to confusion, inefficiency, and frustration across the organization. This will be present among the teams striving to facilitate DevSecOps and the leadership anticipating key business outcomes tied to a successful DevSecOps implementation.

Implementing DevSecOps is no easy task. That said, when done correctly and patiently, while focusing on key competencies, it can reap tremendous benefits for organizations. Not only is there potential for increased rates of delivery, responsiveness to user and market demand and competitive advantage, but there is also the ability to mitigate vulnerabilities sooner, cheaper and far more efficiently than traditionally done. In a society facing rapid digital transformation, the successful adoption of DevSecOps can prove invaluable.

Chris currently serves as the Co-Founder and CISO of Aquia Inc. Chris has nearly 20 years of IT/Cybersecurity experience. This ranges from active duty time with the U.S. Air Force, a Civil Servant with the U.S. Navy and General Services Administration (GSA)/FedRAMP as well as time as a consultant in the private sector. In addition, he also is an Adjunct Professor for M.S. Cybersecurity programs at Capitol Technology University and University of Maryland Global Campus. Chris also participates in industry Working Groups such as the Cloud Security Alliances Incident Response Working Group and serves as the Membership Chair for Cloud Security Alliance D.C. Chris also co-hosts the Resilient Cyber Podcast. Chris holds various industry certifications such as the CISSP/CCSP from ISC2 as holding both the AWS and Azure security certifications. He regularly consults with IT and Cybersecurity leaders from various industries to assist their organizations with their Cloud migration journeys while keeping Security a core component of that transformation.

References


Malware Risks with PIV and CAC Card Readers

John A. Hoeg, BCRC

Several months ago, I received my federal Personal Identity Verification (PIV) card, which I understood would give me appropriate building access, as needed, as well as to serve as an authentication tool when on prem. I was never instructed of any procurement process or approved hardware list. I did a bit of research and found that Amazon had a Saicoo CAC Smart Card reader for $15, which I didn’t mind paying out of pocket to get the device in less than 24 hours. I also felt that I was doing the right thing for the company versus wasting several times that amount in paperwork, approvals, and other administrative red tape.

My Windows 10 system did not require drivers for this plug and play device, but my system was popping up a few occasional errors, so I figured the best thing to do would be to get the most current firmware/driver right from the vendor. I downloaded and virus scanned the zip file and immediately there was a detection of Ramnit.A malware. I immediately contacted the vendor and inquired as to why their driver software contained a virus. Their reply in no way addressed my concern but rather included details as to how to install the file. This immediately set off red flags and I felt like I needed to get the word out through the proper escalation channels. With around 5 million PIV cards out there and this being the number one seller on Amazon, with over 11,000 reviews, there might be significant cause for concern. I saw this as quite possibly the perfect attack vector. By compromising the driver for a device used for multifactor authentication to federal resources, a malicious actor could potentially access a great deal of content.

Unfortunately, after opening tickets and contacting CISA Central, I was offered to receive a replacement PIV card (which was not broken) in addition to being admonished for using one off the internet instead of US government issued card readers. I don’t know if I was more upset or frankly shocked about the willful apathy towards the gravity of the situation. At a minimum, there are potentially thousands and thousands of users actively using these devices with a false, but elevated sense of security by utilizing this extra layer of authentication. I brought these findings to our daily InfoSec team meeting and the consensus was to reach out to Brian Krebs, of Krebs on Security, who is one of the biggest influencers in the cybersecurity field. I sent the details over to Brian and figured that a minion might possibly reach out in a few weeks, if there was any credible substance to my discovery. Surprisingly, 20 minutes after my email, Brian called me directly and after what seemed like a 20 minute espresso fueled dissection of the issue, he felt like this was something worth getting out to the masses. What started as a single tweet to his followers gained some traction and morphed from a 7 part thread to a subsequent feature article which has been translated a few dozen times and made
the rounds in the greater cybersecurity community: [https://krebsonsecurity.com/2022/05/when-your-smart-id-card-reader-comes-with-malware/](https://krebsonsecurity.com/2022/05/when-your-smart-id-card-reader-comes-with-malware/)

On May 31, 2022 a Department of Health and Human Services CCIC Incident Management Bulletin was released as a notification of the details of the threat/vulnerability as well as recommended mitigation actions.

The main takeaway of all this is to practice due diligence when purchasing and installing hardware and software to access both work and personal resources on a network.

Much like the single gate left open that lead to the fall of Constantinople, the blow dealt to the hardware vendor, Saicoo, by the presence of a single, possibly unintentionally corrupted zip file has inflicted insurmountable reputational damage to the brand.

At the end of the day, security is EVERYBODY’S job, not just the various Cybersecurity and InfoSec teams.

*John Hoeg is an Information Security analyst with the BCRC and is a CISSP, CISM, and Certified Ethical Hacker with a 30+ year background covering IT Engineering, Messaging, and Information Security. He is also actively pursuing a PhD in Cybersecurity with a specialization in Governance, Risk, and Compliance.*

**LAPSUS$ Group**

*John Laycock, CCIC*

In March 2022 reports of a compromise around Okta, an American identity and access management company, began to surface. A hacking group known as Lapsus$ claimed they had access to Okta and posted eight screenshots as proof which were shared out by the vx-underground Twitter account. This was the latest in a prolific string of high-profile data breach incidents by the group.
vx-underground Tweet with screen captures of "proof" provided by LAPSUS$ for alleged breach on Okta.

Source: CCIC-CTI

Their hacks date back to as early as May 2021 when they burst onto the scene with data from oilfield services company, Schlumberger. They followed that up with a number of hacks of Brazilian companies. By December 2021, they established a Telegram channel identifying themselves as Lapsus$. Their initial posts were in Portuguese, leading many to speculate they may be Brazilian or Portugal based. As they continued more posts were made in English.

Over February and March 2022, they had claimed data breaches involving Nvidia, Samsung, Microsoft, and Ubisoft. For the Nvidia breach, the Lapsus$ actors claimed to have source code for their chipsets and would publicly release them if they did not open source their driver software and disable Lite Hash Rate (LHR), a crypto-mining performance limiter.

To continue the spree of data breaches Lapsus$ started soliciting on Telegram and Reddit for insiders at various mobile carriers and other companies to help them gain remote access to those companies.

LAPSUS$ group soliciting insiders on Telegram.

Source: CCIC-CTI
The following post was made on Reddit:

![Post on Reddit](image)

LAPSUS$ group soliciting mobile carrier employees on Reddit.

**Source: CCIC-CTI**

Shortly after the Okta announcements, a Twitter user claimed to identify a member of the Lapsus$ group and included a link to a YouTube video. A few days later London police arrested seven individuals between the ages of 16 and 21. One of the individuals is believed to have made a profit of 14 million dollars from hacking and is the alleged ringleader for the group.

**Takeaways**

Threat actor groups will utilize many methods to gain access to sensitive systems. Many times these actors will try to leverage vulnerabilities through unpatched systems or phishing techniques. However, as demonstrated by the Lapsus$ group actors, people should be aware of more targeted solicitations by these actors and report any unusual solicitation posts they may encounter over various social media platforms. Actors may also attempt to contact employees over job related sites like LinkedIn. If you see something or are contacted please report it to the Insider Threat team email, InsiderThreat@cms.hhs.gov.

John Laycock is the contractor lead for the Cyber Threat Intelligence (CTI) team in the CMS Cybersecurity Integration Center (CCIC) and is a lifelong Cubs fan. This information is based on a longer form report prepared by the analysts of the CTI team, Jesse Arredondo, Joseph Tritico, and Malakai Bailey. The team can be reached via the CTI email at CCIC-CTI@cms.hhs.gov.

**CMS Zero Trust Maturity Framework is coming!**

*Elizabeth Schweinsberg, Digital Services Expert, USDS*

Zero Trust is a popular phrase in information security these days and its popularity will continue to grow due to some recent guidance for government agencies. This article provides an overview of zero trust and describes the recent guidance. We also discuss the current plans for Zero Trust at CMS and follow up with some next steps and resources for more information.

As part of the journey to increase the Zero Trust Maturity of CMS infrastructure and applications, the Zero Trust Workgroup has been developing a maturity framework for specific areas of CMS infrastructure. We started with AWS for CMSCloud, and are ready to test out the framework!

In August 2021, CISA released a Zero Trust Maturity Model in draft form, which covers the 5 Pillars of Zero Trust (Identity, Devices, Networks, Apps, and Data) and sets maturity goals across 3 levels -- Traditional, Advanced, and Optimal. This model is a great starting point, and we thought we could enhance it even further by creating specific implementations of it tailored for CMS. There are many different versions we could make,
but since applications written on CMSCloud are going to have the most homogeneous architectures, this seems like a good place to start. We picked AWS because it still had a larger "market share" than Azure within CMS.

By evaluating multiple applications or systems against the maturity framework we can start to find the most efficient improvements to increase Zero Trust maturity, and ideally, reduce the risk and impact of breaches. Initially, we'll be able to identify changes ADOs can make now with existing CMSCloud tools, and over time, we'll be able to see what other tools CMSCloud could use and get them added.

Generally, we're asking the following questions to help us focus on the most impactful efforts in each pillar for CMS:

- Identity -- how do members of the project (e.g., developers) gain access to the infrastructure?
- Devices -- how does the project manage virtual machines and containers (e.g., EC2 and ECS)?
- Networking -- how does the project manage networking within the AWS account and externally, including encrypting data in transit?
- Applications -- how does the project function for users, handle threat prevention, and security testing?
- Data -- how does the project handle data, including access, encryption, and data categorization?

There will be two phases for the AWS on CMSCloud maturity framework -- the trusted testers phase that is occurring now (June 2022) and the regular phase in August and September 2022. For trusted testers, we'll schedule a 90 minute interview to go over aspects of the five pillars as well as collect feedback on the questions we ask. Want to become a trusted tester? Email us at ISPGZeroTrust@cms.hhs.gov!

Elizabeth Schweinsberg is a Digital Services Expert with the United States Digital Service (USDS)

**From the Vault: Continuous Diagnostic Monitoring (Jan-Feb 2019 Issue)**

*Jamal Webster, CGI Federal*

The Centers for Medicare & Medicaid Services (CMS) is a vital part of the overall Human and Health Services (HHS) system tasked with strengthening and modernizing the Nation’s health care system. To support the many HHS programs, CMS extends a portion of innovation and core functions to contractors who bid systems to support larger agency objectives. While the relationship with these external business partners are essential, it is also necessary that these systems are vetted and monitored continuously. Contractors play a critical role in CMS’ security readiness as it adapts to minimize the risks of a dynamic threat landscape by continuous diagnostics and monitoring (CDM).

**Continuous Diagnostic Monitoring (CDM)**

Threat actors have many techniques for footprinting systems to discover high probability paths to exploitation. At the same time, an overarching strategy by organizations such as the National Institute of Technology (NIST) in the reduction of cyber-related risk is information-sharing with the community of practice.
While this vulnerability information offers a clear benefit, it also becomes easier for attackers to overcome the first obstacle of information gathering to determine a path of least resistance for an attack. This creates a scenario where this information means everything to those that maintain systems, as well as those looking to exploit them. To close the gap organizations like NIST are releasing this information to the public and the point in which vulnerabilities are mitigated, we must understand that security is not an end-state, but a continuous dynamic process.

It is very important that Information System Security Officers (and contractor ISSOs) understand the necessity of continuous risk monitoring and its role in situational awareness.

CGI Federal attended the recent 2018 Annual Capital Cybersecurity Summit in Tysons Corner Virginia. Among the various emerging topics related to the cybersecurity industry, one of the keynote speakers called to attention the need to not only collect risk-related data in a timely manner, but also find a way to use it more efficiently as a resource for decision-making. The aim was to gain perspective on the data acquired from the different security resources, and use that information to make pivotal risk-based decisions. This supports changes to the 2014 FISMA requirements where the use of automated tools are being sought to help us shift from point-in-time to real-time assessments where data is being pulled from more places more often than ever before. As processes continue to move towards continuous authorization, ISSOs must be prepared to take a slightly different approach to security where there is enhanced transparency for the stakeholders of the system. With CMS’ CDM implementation, a variety of Security Information and Event Management (SIEM) endpoint tools and sensors are leveraged to facilitate data aggregation at a faster frequency. Contractor ISSO’s will have an integral role in seeing that vulnerability and compliance information collected by the CDM implementation is promptly presented to project teams triggering the necessary remediation efforts.

The Paradigm Shift and the Role of the Contractor ISSO

While change can be met with reluctance, ISSOs must use their influence to enable the paradigm shift where continuous monitoring is implemented and refined. They must ensure that it is not only understood to be a requirement, but also a fundamental necessity commanding commitment both internal and external to CMS with buy-in from the top down. This must be achieved via knowledgeable ISSO’s that are intrinsically motivated to make a difference and understand the advantage of real-time vulnerability data. The future of risk management demands that security professionals adapt to the rapidly changing atmosphere of information assurance. Collaborative partnerships between CMS and its supporting contractors may be the practice that gives the agency and all its stakeholders the advantage in developing systems that meet the needs of the public to securely achieve its core mission.


From the Vault: The 5th Generation (5G) Networking Evolution (June July 2020 Issue)

Eric Brockman and Omiome Olaghere BA, MS PhD, CAP, Assyst

The ISSO Journal welcomes first time contributors Omiome Olaghere and Eric Brockman. They provide current information on new 5G technology. In this article they present new wireless technology, and discuss the importance of understanding it.

The top cellphone carriers are no longer providing fast enough data access for their customers; the need for a faster wireless network is here. The move from Third Generation wireless technology (3G) and Fourth Generation wireless technology (4G) is needed for faster and more abundant bandwidth for the exponential
use of internet of things (IoT) capability. The expansion of networks to 5G to meet the need for faster speed, requires technical changes to the existing 3G and 4G networks. The technical designs of this new standard demand high network density to provide the anticipated stratospheric speeds. Understanding 5G networking, wireless security, and the advent of IoT and the role these technologies will play as remote working becomes the norm, and how to protect against potential threat actors, has become essential in our role as cyber security subject matter experts (SMEs).

As remote working becomes the norm, data transfer and secure communication are more exposed to cyber risk and networking vulnerabilities. Additionally, as IoT continues to grow and become more a part of daily life, new ways of thinking about security protection must become prevalent in the cyber security domain. Clare Duffy of the Cable News Network (CNN) Business, reports that 5G is the next generation of wireless network technology for the country. The main focus of the roll out across the country is to create a network that provides faster data processing speeds with greater network capacity than currently provided by 4G technology. A description of the technology being used to build the 5G network is quite similar in premise to the 4G Long Term Evolution (LTE) network currently in use, and follows the same transition as from the First Generation Wireless (1G) to the 3G and now the 5G transition and use of technology. Like preceding technology, 5G uses the radio frequency spectrum for wireless devices to communicate within the cell network. 5G no differently than preceding networks such as 3G and 4G. The difference is that 5G network has the ability to access a wider range of radio frequency. This wider range of frequency gives way to a larger range of bandwidth and speed to access this bandwidth, which is an improvement from the current 4G.

With the current advancements and introduction of IoT, 5G is more of a necessity than an optional technology. IoT, as described by Wikipedia, “is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction”. Having the increased amount of bandwidth also applies to the internet use of other technologies such as autonomous vehicles, smart manufacturing and smart cities. To meet the increase in demand for bandwidth and speed, 5G is available in three forms: low, mid and high band. All three forms of 5G provide very fast transmission and communication. This is primarily due to the signals used in 5th generation transmission technology not having to travel very far. The current rollout of 5G encompasses the majority of the country being equipped with a combination of low and mid band levels, while reserving the high band levels for urban and city areas such as New York, Philadelphia, Washington, D.C. and Los Angeles, to name a few. Interestingly enough, no matter if the area in question has high or low band service, the network for 5G operates at the same frequency, providing the faster access for transmission of data. This increases reliability and also productivity for the users.

Duffy further explains that some of the negative concerns of 5G are dispelled from the research and recommendation of Vytenis Andriukatis of the European Commission (the executive branch of the European Union (EU)) and other experts. Andriukatis’ research reveals that side effects of 5G exposure does not increase health concerns such as cancer; however further research is needed and the health contributors by electromagnetic waves in humans should be noted. There is less controversy around low and mid-level 5G networks as it does not expose humans to any more electromagnetic waves than the current 3G or 4G networks. The network of concerns to health risks is the high band that will be frequently used in large urban cities. University of Pennsylvania Professor Collins states the following in regard to 5G: “…electromagnetic waves penetrating human skin exists at such low levels that it is no different than the waves encountered in the airport scanning machines currently in use by the Transportation Security Administration (TSA)”. The overall concern at the moment is that testing is negligible to rule out the negative effects of 5G transmission
of electromagnetic waves. Current research data is currently reporting minimal side effects to humans when in close proximity to the 5G network.

Another point of concern for the 5G network is the overall implications of IoT. What once were one-way communication devices, such as the clocks set on a table or desk and gave the time without much human interaction, telephones that once hang on the kitchen wall and ring a bell letting you know that someone was on the other line and expecting to communicate, have become “smart” devices, meaning that they are capable of processing data and communicating in very sophisticated ways. This is prompting an evolution of smart devices that are flexible, smaller, mobile and able to connect and communicate to the internet. Currently, cars with engine problems communicate with a light on the car’s dashboard indicating it is needed to be taken into a mechanic and hooked up to a diagnostic machine, showing problem codes that only trained mechanics understood. Now, smart cars connect to the Internet and transfer problem codes directly to the owner and mechanic. Regular household appliances, such as stoves and refrigerators are now smart devices and connect directly to the Internet, transferring data back and forth with computer systems and other smart Internet connected devices. These devices and appliances pose the greatest risk to Personal Identifiable Information (PII) and Personal Health Information (PHI) since they are designed around weak authentication, come with default credentials that are never changed, communicate via unencrypted messages sent between devices, are susceptible to SQL injections and poor handling of security patching updates. These devices and appliances can be subverted to attack other systems, such as computer networks and computer systems.

Ensuring that the upgrade to 5G networks has the appropriate and applicable security policies and protocols in place is of paramount importance in protecting the PHI and PII from threat actors, when transmission occurs by smart devices over the internet. Fortunately, securing and protecting data communication traffic is not a new concept in that security professionals have been applying a risk based approach for several years to critical systems, using the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 (currently Revision Four) security control guidance to implement, secure, and protect data at rest and data in transit. In essence continued and applied use of the Confidentiality, Integrity, and Availability (CIA) triad and the Risk Management Framework (RMF) process will help ensure information in transit and the systems it touches are secured from treat actors.

In summary, the Information System Security Officers (ISSOs) need to be familiar with the security characteristics of the underlying technologies and components of the supporting infrastructure required to effectively operate a 5G network. In particular, the CMS systems that have Internet access capability and mobile device connections or cloud technologies must meet industry compliance requirements for 5G network use, as the security implications of device connections to cellular networks must be leveraged with current and future NIST guidelines. Becoming familiar with the guideline can help CMS ISSOs remain on the cutting edge of information security.

References
2. Bartock, M., Cichonski, J., and Souppaya, M. (2020 April 22) 5G Cybersecurity, preparing for a secure evolution to 5G NIST Journal online article.
4. Internet of Things (June 30th 2020) Wikipedia article.
Eric Brockman and Omiome Olaghere provide assistance to Cyber Risk Advisors (CRAs) in CMS’ “CRA As a Service” contract. They both are with Assyst.

ISSO Open Mic
ISSOs have volunteered in some cases, and we have asked in others, to let us know their thoughts on issues related to the ISSO experience at CMS. This edition’s topic was raised during the CMS Information Security Advisory Board (CISAB) meeting held in March 2022. In that meeting senior ISSO Kevin Allen Dorsey asked questions from his peers about their experiences with Penetration Testing (Pen Testing). He was curious about ISSOs’ experiences with training, preparation and execution. Accordingly, we asked the Community:

- How do ISSOs find out or get training on CMS procedures for penetration testing?
- How often are penetration tests performed?
- Which environments are penetration tests performed in?
- Is anything being done with CMS/MITRE tools such as Synthea?

ISSO Esmail Essajee responded:

Our last round of Pen Test, for the CDAT-M system, was conducted last year. Our experience was both interesting and frustrating. Interesting in that the contractor, Synack, has retained “researchers” from all over to assist them with the Pen Test. A team is selected from the very many list of “researchers” who then Pen Test the system in many different ways. Also, all communications, results and findings during and after the Pen Test was done using the contractors webtool which was new to us. Hence, there was a “learning curve” involved.

Setting up their Account Provisioning was the frustrating part. We had to setup the “generic accounts”, disable the MFA and provide training to ISPG staff who in-turn trained the “researchers”. When the “researchers” tried to login they were getting various error messages. We then had to work with them independently to get them onboard. This caused a small delay to the start of the Pen Test.

All said, the Pen Test went well with no Critical or High findings. Working with Synack was pleasant as they were very responsive and cooperative.

We have another Pen Test scheduled with them for this July and look forward to another successful venture with Charles Gomez and his team at Synack.
Editor’s Note: This conversation began to touch on another conversation about the proper environment for Pen Tests to take place. There was brief mention of Synthea, a tool/project which will help solve the problem of having good data for pre-production. This project is something that all ISSOs might find interesting.

Are You a New ISSO, Or Do You Know One?

John Myers, Assyst

In Issue 19, we reviewed some of the tools that the ISSO Workforce Resilience Program has made available for ISSOs. We talked about the Score Card, Mentorship Program, and tools including the ISSO Guide and the ISSO Welcome Packet. Since then we have received requests for a mentor, and have fielded questions about information for new ISSOs. It has prompted us to suggest a way for new ISSOs to use some of the tools that we have available.

People come to the ISSO role from various backgrounds, with differing levels of experience. Even cybersecurity professionals need to learn the “CMS Way” of doing business. They need to learn CMS workflow, quirks, governance, and undocumented ways of proceeding. Those with less cybersecurity training and experience face an additional hurdle of understanding cybersecurity concepts.

Rather than figure out how to use the tools that have been provided, we suggest using a common approach, no matter what your background is. Follow a five-step process to:

1. Determine what information you already know and what information you need to either learn or brush up on via the ISSO Score Card
2. Based on your results from the Score Card, take some of the appropriate video courses from the ISSO Fundamentals Series (https://www.cms.gov/CBT/Forms/Isso.aspx). There are six videos that address all aspects of an ISSO’s job requirements. You can take one or two as needed; we suggest all six;
3. Sign up for CFACTS Training. Yes, CFACTS Training is still around. For old hands who remember it as a hands on course, things have changed. Although no longer hands on, it is now two pretty full days of CFACTS training that demonstrate a detailed introduction to CFACTS through the prism of the Risk Management Framework.
4. Finally, use the custom training plan that you received from the ISSO Score Card. This will give you a targeted list of training and education opportunities custom made for you.

If you are a new ISSO, we suggest that you try this approach to ‘snap in’. If you know a new or prospective ISSO, we suggest that you point them in this direction. Finally, don’t forget the ISSO Mentorship Program.
(This is step 5). No matter how good or thorough documentation is, it is always helpful to have someone to turn to for help. If you want to have a mentor, send a note to ISSO@cms.hhs.gov with the word Mentor in the subject line.

Thanks,

The ISSO Support Team

What’s HOT?

The good news is that things are not static around CMS as they relate to Cybersecurity. The better news is that there is a LOT of communication in the form of meetings, Slack Channels, Confluences, Zoom calls, etc. Sometimes it is helpful to know what to look for with the many invitations available. While we try to invite subject matter experts and project managers to write in the ISSO Journal about their programs, we want to highlight and point to some of these communication efforts. What’s HOT is a new feature that points out some of the programs that are in development and are worth looking into, if you are not already involved.

- The Rapid ATO Project, combined with Ongoing Authorization, are areas that are essential for ISSOs to understand.

- Batcave, although designed to “shift security left”, is important for ISSOs to understand both in the execution of their duties and to be able to explain to Business Owners.

- CFACTS improvements and upgrades are occurring at breakneck speed. It is vital for ISSOs and security contractors to stay dialed in with this process, as new changes and decisions are made every week. Make sure that someone from your team is on the CFACTS call each Friday at 10:00 AM.

- How many CMS systems struggle with developers’ absolute “needs” to use Prod Data in pre-production environments, with the inevitable pushback against including these environments in the authorization boundary. The answer is, just about all of them! Synthea is a product designed to offer very real data for dev/test/val without the security requirements. If you haven’t heard of this project, look for Synthea.

- SIA update project, an exercise in ‘continuous process improvement’ is being refined and updated.

- Workforce Resilience Project is an ambitious, far-reaching project that impacts all of CMS and transcends cybersecurity training. Look for meeting and Zoom opportunities here.

- Cyber Risk Management has a wonderful, customer-centric approach to communications. There are numerous opportunities, meetings, Zoom calls available.
We will add more to this list as they come up. We do not want to replace or “talk for” any of these programs. Our goal is to help make you aware of their presence.

Gaining Access to HHS Resources
Lawrence Grim

Have you seen a reference to HHS’ Information System Security Policy (HHS IS2P) and found that is not posted publicly? Lawrence encountered this problem and successfully navigated the system to gain access. He has documented his steps for us.

1. Go to the HHS Intranet page, at https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/policies

2. Navigate down the page to the HHS IS2P entry

3. On the MAX login page, put in your CMS email and password you setup with the MAX system
4. The MAX login will prompt for a more secure login with your PIV card. Not having one at this time, I declined to use a PIV card.

5. Then, the popup window asked for what was to be done with the PDF download. I actually requested to save it to my local drive.

6. The location chosen was my Document folder.

7. Document download finished and virus scan was completed.

8. Selecting Open has Microsoft Word open in Compatibility mode and show the document. Note the document is the newer DOCX rather than DOC, which protects against malicious macros.
9. To get any updates, return back to the HHS OCISO policy page and get the updates

10. This will open up a new page to download the addendum

11. When the page opens for this PDF, move the cursor to the bottom of the page. The PDF controls will be provided to allow the PDF to be saved.
Larry Grim is a senior Cyber Risk Advisor (Contractor) with ISPG

Cybersecurity Community Forum Notes for April and May 2022

On April 5, 2022:
- There was a detailed CyberVets update

On May 5, 2022:
- John Myers discussed the ISSO Score Card
- David Wheeler discussed ACT and the “Risk Assessment” Pilot
- Gita Ollange discussed the updated Vulnerability Monitoring Dashboard

Access/Questions
If you are not on the email list for Cybersecurity Forums, send a note to isso@cms.hhs.gov. Your name will be added to the list.
Data Guardian Update
Eric Larson, IRIS Health Solutions, LLC

Data Guardians are staff who, representing their Centers and Offices, ensure a coordinated and consistent approach to protecting personally identifiable information (PII) and protected health information (PHI) across the CMS enterprise. They support an information security and privacy awareness culture, federal policy, standards, and requirements that apply to protecting CMS’ data and assets. The following synopsis presents minutes from the past two monthly meetings.

Adjusting Meeting Frequency
Leslie Nettles

It was asked if meeting monthly was necessary and if the DGs think the team can accomplish the same responsibilities meeting quarterly as a group and in the between months use email or slack communication channels. Also, one off, impromptu meeting can be called by any DG if there is a situational need. The DGs voted to give the new schedule a chance to fail or succeed.

Combatting Insider Threats within CMS
Daniel Browne, John Laycock, & Jeremy Tippett

John introduced himself as the lead for the Cyber Threat Intelligence and Insider Threat teams. He also introduced two members of his team and today’s presenters, Jeremy Tippett and Dan Brown. The presentation will focus on lessons learned and review a few real-world examples of how destructive an insider can be to an organization.

Dan defined what an Insider Threat is and that 60% of insider incidents are caused by negligence and not following security protocols put in place by the organizations, i.e., Human error. He reiterated that employees or contractors are a greater threat because they have access within the firewall of the organization and can introduce malware to the network and more importantly steal or delete proprietary information and organizational secrets, that can be devastating to companies causing down time, IT damage and clean-up/reconfiguring that can cost millions. Not to mention the lack of business associates trust that can come from a breach of any company’s security.

Jeremy Tippett provided three examples on insider threat, (two malicious and one not):
1) There was a case that involved a well-known US based Telecommunication company where the subject was the primary liaison for foreign government law enforcement and intel services. This individual was utilizing his position to bypass security and pass sensitive information to foreign governments. This case was eventually investigated by the FBI.

The lessons learned from this case is that human resources, system business teams and security must have clear lines of communication and work collaboratively to follow up on incidents before they escalate into something that does real harm and becomes a media story.

2) The second example was concerning an ex-employee of a Californian-based company who prior to leaving the company created a backdoor into their system. Later while at home, he logged into his old company and delete approx., 1,200 Microsoft Office email accounts from their system. The company have no emails account or historic emails and customer point of contacts. It caused the company to shut down for over a week and four weeks to remedy the situation costing a million dollars in damages.

The lesson learned here, if that employee was not escorted out when terminated and was allowed to go back to his office to clean it out, where the former employee created a user name and password to access the system.

3) In the case of a non-malicious insider. The team has found that one of the biggest obstacles is when an employee accidently clicks on a phishing campaign but then does not let security team know out of embarrassment as no one really wants to admit they fell for a scam. John advised everyone to just be honest and let security know. Remember if you see something suspicious let the security and the CMS SOC know.

If you have question or concerns please email the InsiderThreat@cms.hhs.gov, even if they cannot help, they are able to route the concern to the correct department to act.

Understanding the Risks of Federal Foreign Travel

Jeremy Tippett

The team has learned a number of things concerning foreign travel. Most important is that data privacy laws in the United States are very different from the data privacy laws in foreign countries. HHS and CMS take this very seriously.

1) No employee is authorized to take their issued CMS Laptop or iPhone outside the United States.

2) If an employee logs into a hotspot from Canada, the CMS Cybersecurity Integration Center (CCIC), Security Operation Center (SOC) will get pinged from that foreign server and action will be taken. Please tell your staff. Unauthorized foreign travel also violates HHS Rules of Behavior.

3) Employees that are authorized foreign travel will be issued a GFE loaner phone and laptop that is cleaned/scanned upon returning.

4) Foreign countries have the capability to wirelessly access phones and install malware. You might remember the warning to Olympics athletes heading to China for 2022 winter games. It was strongly suggested to leave personal phone at home and buy disposable phones/burners.

5) John and team thanked the group and reminded folks that any individual who has C3 status or a security clearance must report any personal foreign travel.

6) For additional questions on Foreign/international travel, please email intenational@cms.hhs.gov;

Phishing Results February 16 – 19

Eric Larson
This campaign did not have as many obvious clues as the last months phishy email did. The email was from @cms.hhs.gov domain, but the name was not in the global and the end user should ask themselves if they should be receiving this email and if they ever had in the past.

The results of the campaign are:

- 10,144 recipients phished
- 3525 reported
- 1781 opened the emails only
- 204 clicked (phished)

CMS must increase the difficulty of the phishing campaigns because our advisories are making the phishing campaign more authentic looking. Remember to pass on to your components, if you are in doubt of an email, phishing it out by reporting it, via the Report Phish ICON in MS Outlook. DO NOT Delete the Phish, Report it.

---

**Eric Larson** provides support for Privacy and Data Guardian tasks within ISPG

---

**CMS Information Security Advisory Board (CISAB) Update**

*Cole Schencke, Assyst*

The CMS Information Security Advisory Board (CISAB) was established to provide a mechanism for cybersecurity and privacy concerns between the CISO, the Information Security and Privacy Group (ISPG), and CMS Information System Security Officers (ISSO). CISAB is a conduit for ISPG staff and ISSOs, both federal and contractor, to regularly collaborate and exchange information concerning cybersecurity and privacy related material and knowledge.

In our April meeting, our cohort discussed the objectives of a pen-tester as well as tools they use to conduct pen-tests like Synack. Our May meeting saw a brand-new cohort consisting of experienced ISSOs and new ISSOs as well as returning CISAB members and fresh faces. We discussed whether or not the ISSO role had national security implications as well as the difficulties CMS is facing from hackers using offshore IP initiation requests to reach different systems at CMS. If any of those topics sound interesting to you, you can find audio transcripts of our previous meetings on the CISAB Confluence Page. Consider joining our Slack channel #cisab for updates.
Our June CISAB meeting will be held June 22nd at 11AM. We look forward to seeing you there.

*Cole Schencke is a contractor working within ISPG on the ISSO Workforce Resilience Project. He has recently taken over Secretariat responsibilities for the group.*

**Training Update**

*Saad Zulqadar*

**Getting Your Role-Based Training Requirement Completed**

For those of you with Significant Security Responsibilities (SSR), you are required to complete annual Role-Based Training (RBT) that aligns with your role assignment.

To help you easily meet your requirement, check out our new training course, *Risk Management and You*. This quick course covers all NICE-based cyber codes and can be found at [https://www.cms.gov/cbt/Forms/Home.aspx](https://www.cms.gov/cbt/Forms/Home.aspx). Please complete this training no later than **July 12, 2022**.

In addition, watch for the **new Information System Security & Privacy Awareness (ISSPA) course** later this year. It will include an RBT module that will also satisfy your RBT requirement for the year.

*For more information on CMS RBT, take a look at the Information Security & Privacy Training Catalog. Here you can find dozens of training opportunities, many that are aligned to the NICE Framework to meet RBT requirements.*

*For questions concerning SSR, please reference the Information Systems Security and Privacy Policy (IS2P2).*

**New Two-for-One Training Deal!**

We are excited to announce that the new Information System Security & Privacy Awareness (ISSPA) course will soon include a new Role-Based Training (RBT) module and will be available this fall. That means taking this **new ISSPA course** will also satisfy your RBT requirement for the year! Now that’s a two-fer you won’t want to miss!

*For more information on CMS RBT, check out the Information Security & Privacy Training Catalog. Here you can find dozens of training opportunities, many that are aligned to the NICE Framework to meet Role-Based Training requirements.*

*Saad Zulqadar provides training expertise and experience to ISPG with cybersecurity training.*

**Internal and External Resources for ISSOs**

**Confluence Sites**

*ISPG ISSO Workforce Resilience Program* (Confluence) This Confluence presence is replacing the ISSO SharePoint site.

*ISPG Policy Initiative Team* (Confluence)

**Slack Channels** – Slack is the collaboration hub that brings the right people, information, and tools together to get work done. ISPG currently sponsors security Slack channels you may want to join and we are always open
to being invited to channels you finding interesting. you must install the Slack app on your laptop to access Slack and these channels.

Below are just some of the channels available:

- #cra_help (71 members)
- #security_community (278 members)
- #vulnerability-digest (73 members)
- #ciso-bookclub (20 members)

For ADO ISSO’s... #cms-cloud-security-forum (174 members)
For ISSOs... #cms-issos (158 members)
General topics... #General (7,614 members)

Web

- [NIST Cybersecurity Framework](https://www.nist.gov/cyberframework)
- [NICE Cybersecurity Workforce Framework](https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework)
- [US-CERT](https://www.us-cert.gov/)
- [SANS](https://www.sans.org/)
- [OWASP](https://www.owasp.org/index.php/Main_Page)