CMS ISSO Journal

...by and for CMS Cybersecurity Professionals

July-September 2023

Issue 25

CMS ISSO JOURNAL

July-September 2023 Issue 25

Highlights

Welcome to the second edition of the *CMS ISSO Journal* for 2023! This edition has several interesting articles and features, many of them of particular and immediate interest to ISSOs and their staffs.

- Want more insight on what it's like to be a CRA here at CMS? Find out more in **A Day in the Life of a CRA**.
- **Getting a Pentest? Try a Threat Model first!** Learn more about Threat Modeling and how it can benefit you during a pentest!
- Need a refresher of what Vishing is and how it can affect you? Read **What Is Vishing and how to Protect Yourself Against it** to find out more.
- These are just a few of the many important and interesting things found in this edition. Happy reading!

The CMS ISSO Editorial Staff

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

Read the Journal online at ISPG ISSO Workforce Resilience Program (Confluence).

Journal Contents

Data Guardian Update

Eric Larson, MITRE Corporation

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 quarterly meetings.

Next meeting – November 15, 2023

Project D20

Jay Shao and Doug Nock

Jay informed the Data Guardians that he works with Doug Nock as part of the Mission Enablement (ME) team at ISPG. The ME team scales secure and proven products and services to enable teams across CMS to achieve their goals quickly and safely, while strengthening the IT security posture. One of their main projects is building out the CMS Security Data Lake platform.

With Project D20, the ME team is working to understand the various challenges of conducting tabletop exercises at CMS to identify opportunities to improve the tabletop exercise experience, with the overall goal to encourage more ISSOs and Business Owners who may be hesitant to engage in tabletop testing exercises to do so. Project D20 would like to understand how we can:

- make tabletop testing more budget friendly?
- make testing easier to conduct with or without a facilitator?
- make testing less formal, require minimal preparation, and complete in less than hour?
- build out ready-to-go scenarios based on CMS threat intelligence?

The ME team contacted Business Owners and ISSOs in CCSQ and CCIIO, inquiring how they conduct tabletop exercises in the past. The team received positive feedback, but the data is inconclusive. Consequently, D20 is seeking additional input to make better, informed decisions on the path forward and ask ISSO's and BO's to please complete the short survey https://cmsgov.typeform.com/to/R7ohiQsm
If you have questions contact Jay Shao, justin.shao@cms.hhs.gov and Doug Nock douglas.nock@cms.hhs.gov

Phishing Training Program Update

Don Bartley & Patrick Laverty

Don and Patrick provided an update on the August Phishing
Campaign. This campaign is the first to be extended from one week to two weeks (a full 14 days), allowing more time for staff to respond. The program will continue this process, analyze the results, and include in the next report provided.

Patrick reminded the team that the Social Engineer, LLC (SE), pilot project started in November last year and they are on their 10th monthly phishing campaign, that:

- Uses a levelized phishing program as they send three different difficulty levels of phish. The difficulty level of the phishing templates increases in complexity as staff successfully reports the phishing emails. If the staff does not report, they will continue to receive level one (lots of phish clues), or level two difficulty phish (less clues), and will not advance until they prove they have learned to identity and report the phishing emails. Level three phish of course looks very real with minimum errors in text, sender information or format.

Acknowledges the positive, focusing on contacting those individuals who reported the phish properly, as well as those who did not interact with the phish. The CMS/SE phishing program does not focus on those who became susceptible. However, these individuals are not ignored. When someone is phished, they receive a screen popup notifying them and displaying the email with the clues pointed out. The objective is to educate on the spot. Then the staff member is phished again at the same difficulty level until they pass to the next level. June's campaign reflected a low 31% of staff identified and reported. The team's assumption is that that staff was away on vacation as the number doubled for July's campaign. Of July's 4448 level three emails sent, 61% identified and reported the phish. August's Campaign will close next week and will be reported at the November 15 Data Guardian meeting.

Reminder, the success of the program hinges on the number of individuals who properly report the phish rather than ignoring, forwarding, or deleting it. SE aims to cultivate "the ideal behavior" among staff members, encouraging them not to click on or interact with malicious emails.

Data Guardian Handbook Introduction

Leslie Nettles and Eric Larson

The Data Guardian handbook can be found, via the CyberGreek webpage located at https://security.cms.gov/ From that main page, you can access the handbook by scrolling down to Role-based information section and click Data Guardians.

The handbook's page is updated to reflect the various means contactors and federal staff access CMS email and how to report any suspicious email.

- For MAC Users and Federal staff using the browser version but forward phish to spam@cms.hhs.gov.
- MS Outlook Users should download/install the Report SPAM/PHISH icon adding to the MS outlook ribbon.

Phishing Hall of Fame

Eric Larson

The CMS Phishing Hall of Fame, updated monthly, recognized staff members who reported real-world phishing attempts. Between January and July, CMS staff reported **719** real world phishing. The hall of fame is updated monthly, (HOF Link). August inductees will not be reflected until the first week of September and with have that month's inductees **bolded** to better identify those who reported real threats to CMS's network. Please see the Phishing Hall of Fame for inductee's name and please congratulate them for a job well done!

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

ISPG Division of Strategic Information SCRM Team Provides Support for Mandated Training

Thomas Hobert

A memo issued July 17, 2023, requires all HHS acquisition workforce members complete an e-learning course, FAC 093, Introduction to Supply Chain Risk Management, before November 14, 2023.
The course, FAC 093, Introduction to Supply Chain Risk Management, provides an understanding of SCRM including common terminology, best practices, safeguarding sensitive information, general prohibitions, exclusion orders, and additional requirements for higher risk procurements.
This course is available at no cost through Federal Acquisition Institute (FAI) Cornerstone on Demand (CSOD); a direct link to FAI CSOD is available here: https://dau.csod.com/. The course is comprised of two parts – an interactive, narrated e-learning course and a 10-question multiple-choice quiz. The total time commitment is approximately 60 minutes.

Accessing and completing this course requires a Defense Acquisition University (DAU) account. If HHS acquisition workforce participants do not already have DAU accounts, when they click the Federal Acquisition Institute (FAI) Cornerstone on Demand (CSOD) link, they will be prompted to complete a form requesting an account be established.

The process may take several days and participants are encouraged to plan ahead to avoid last-minute problems.

When the account access form is completed, submitted, and granted, participants will receive an e-mail notification.

If that e-mail notification is not received in 3 days, reach out directly to DAU Help Desk at 703-805-3459.
The ISPG DSI SCRM Team is actively supporting the HHS acquisition workforce. That support has included

formal presentations with question-and-answer sessions with the Office of Acquisition and Grants Management (OAGM), but the SCRM Team is also available to assist HHS acquisition personnel on a consultative basis as well as *ad hoc* questions and support. The SCRM Team hosts Supply Chain Risk Management Library – or they can be reached by e-mail at SupplyChainRiskManagement@cms.hhs.gov.

Michael Hobert is a Consultant with LMI where he is focused on Supply Chain Risk Management training, outreach, and awareness. He has a broad background in training, education, and skills development. Michael has worked in tech, finance, and healthcare for top Fortune 500 companies as well as disruptive start-ups. Despite the diverse background, he says what he does is simple, "I make complex ideas, information and skills accessible to diverse audiences."

Getting a Pentest? Try a Threat Model first!

Maril Vernon (Aquia)

Introduction

As the sports saying goes, "The best defense is a good offense." The idea is to gain a strategic advantage against an opponent by anticipating their move and forcing them to be in a defensive, reactive state. The same applies to cyber security. With the age of cloud, Agile SDLCs, and ever-increasing attack surface, it has become imperative for businesses to embrace proactive security practices to effectively safeguard their assets and systems. Often done alone, two vital approaches in this regard are Threat Modeling and Penetration Testing. But by combining these two practices, organizations can create a powerful cycle that enhances their security posture. In this article, we will explore the concepts of Threat Modeling and Penetration Testing and highlight how they work in synergy together.

Threat Modeling

Threat modeling is a systematic approach to identify and mitigate potential security threats to a system. The process typically follows the well-known Shostack 4-question model, which helps guide the analysis:

- What are we working on? | What is being built and how does it work?
- What can go wrong? | What are the potential opportunities for threats to be realized?
- What are we going to do about it? | Can suitable countermeasures be developed to mitigate the threats?
- Did we do a good enough job? | Regular evaluation and validation of the threat model to ensure that it remains robust and effective over time.

The benefits of threat modeling are significant. It enables organizations to identify vulnerabilities early in the development process, prioritize resources on critical assets or most at-risk assets, and implement targeted security measures.

Penetration Testing

Penetration testing, often referred to as simply 'pentesting' or ethical hacking, is a controlled attempt to exploit vulnerabilities within an organization's systems. It follows a well-defined methodology to simulate real-world attacks and assess the effectiveness of defenses.

The penetration testing process typically includes the following steps:

1. Planning and reconnaissance: Gathering information about the target systems and identifying potential entry points.
2. Scanning and enumeration: Using specialized tools to scan for vulnerabilities and enumerate the exposed services.
3. Exploitation and gaining access: Attempting to exploit the identified vulnerabilities and gain unauthorized access to the system.
4. Post-exploitation and maintaining access: Once access is gained, testers explore the system further to assess the extent of potential damage (impact) and evaluate the system's resilience against attacks.
5. Reporting and recommendations: Documenting the findings, including vulnerabilities, exploited entry points, and recommendations for remediation.

Penetration testing serves as a crucial validation mechanism for the effectiveness of the threat model. There are inherent limitations of a pentest, however:

1. Time: Testers generally only have 1-2 business weeks to attempt as much as possible. Given there is no specific objective, they must first figure out what they're working with systems-wise, identify the vulnerabilities to test, develop the exploits, and test them. This can include database, network pivot, IAM, cloud, web application, container, Active Directory, etc. So pentesters have a noticeably brief time in which to 'throw the kitchen sink' at a system to find as much as possible.
2. Resources: pentests can be costly and as a result generally only happen once annually, which is not an effective cadence to test system changes. Additionally, there may be only 1-2 testers assigned to the engagement. That is a very limited number of resources to effectively test defense-in-depth.
3. Findings: The goal of a pentest is to find as much as possible to maximize the number of possible remediations, but this can lead to anywhere from 30-80 findings in a single engagement. This can result in overload for remediation teams who will never work their way through the backlog with the combination of active alerts.
4. Initial Access: Most pentests do not do white box or 'assumed breach' testing in which they're given audits, network diagrams or local user access to focus their efforts. Instead, they do black box testing which means much of that precious two-week period is spent on getting past firewalls and EDR solutions. This tests the effectiveness of the first line of defense but does not qualitatively address second or tertiary defenses such as RBAC, privilege levels of access, database security, and so on.
5. Scope: Scope is often limited for large environments. Organizations with more than 150 users and endpoints, not including assets such as databases, servers, storage, warm and cold sites, gateways, etc. mean the testers must pick and choose what they're able to accomplish in their short engagement time. It is impossible for a single pentest to identify every possible vulnerability and remediation.

The Synergy of Threat Modeling and Penetration Testing

The true power lies in the combination of threat modeling and penetration testing in a continuous cycle. Some benefits of this integrated approach include:

- Early identification of vulnerabilities: Threat modeling helps focus penetration testing efforts on critical assets, maximizing the efficiency of the testing process. The pentest, in turn, validates vulnerabilities identified through threat modeling alone and provides valuable insights into the system's overall security.
- Validation of mitigation strategies: Penetration testing also validates and verifies the effectiveness of mitigation strategies developed during the threat modeling phase, ensuring they hold up in real-world scenarios.
- Continuous improvement: The feedback loop created by penetration testing results informs and improves the threat model, allowing for ongoing enhancements to the organization's security posture.

Integration and Collaboration

To fully leverage the combined power of threat modeling and penetration testing, collaboration between threat modelers and penetration testers is essential.

A. **Assumed breach and defense-in-depth:**
   Collaboration embraces the concept of "assumed breach," acknowledging that adversaries may already be present within the system. This approach ensures that the organization's defensive strategies are not solely focused on preventing initial access but also on detecting and mitigating threats beyond the perimeter.
B. **Effective communication and information sharing:**
   Close collaboration between threat modelers and penetration testers facilitates the influence of secure design decisions and the validation of proposed countermeasures. By sharing knowledge and insights, both teams can enhance their understanding of the system and strengthen security measures.
C. **Integration into the software development lifecycle:**
   By incorporating threat modeling and penetration testing into the software development lifecycle, organizations can achieve several benefits. They can save costs by identifying vulnerabilities early, save time by proactively addressing security concerns, and expedite remediations by focusing efforts on specific areas rather than reviewing extensive code.

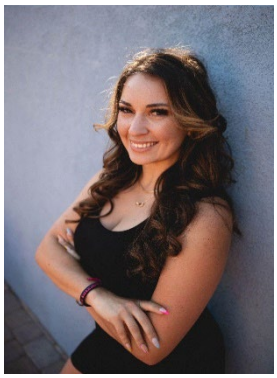
Conclusion

Combining threat modeling and penetration testing creates a powerful symbiosis that strengthens a system’s overall security posture. By leveraging the insights gained from threat modeling and validating them through penetration testing, organizations can identify vulnerabilities early, implement effective countermeasures, and continuously improve their security defenses. Embracing collaboration between threat modelers and penetration testers and integrating these practices into the software development lifecycle leads to more robust and resilient systems.

Learn more about Threat Modeling at CMS:

1. Check out the CMS Threat Modeling CyberGeek page: https://security.cms.gov/learn/threat-modeling or Confluence page (training, videos, etc.): https://confluenceent.cms.gov/display/CTM/
2. Join the #cms-threat-modeling channel on CMS Slack
3. Email the CMS / CASP Threat Modeling Team: ThreatModeling@cms.hhs.gov to receive information on live interactive training or to engage in a Threat Modeling session.
4. Register for a monthly CASP Threat Modeling Office Hours session: First Thursday of the month at 1:00 PM ET https://confluenceent.cms.gov/display/CTM/Threat+Modeling+Office+Hours

CMS / ISPG CASP Threat Modeling Team - Robert Hurlbut, Marial Vernon
CMS / ISPG CASP Lead - Eric Rippetoe
CMS ISPG Contacts - Mike Kania, Robert Wood



Marial Vernon (Aquia) is a Senior Application Security Architect on the CMS / CASP Threat Modeling Team

A Day in the Life of a CRA

Eric Brockman

With many of us here at CMS working remotely for over three years now, it is very important to stay connected and promote better remote relationships for a healthy work environment. Zil Zukhruf Sheikh, an ISSO working in OIT, had the wonderful idea of reaching out to our coworkers and asking them to share information about themselves so that we all stay interconnected and thus improving our work experience. In our first ever interview, we asked Eric Brockman to tell us about himself and his experience in the role as a CRA.

What would you consider as your greatest achievement so far here at CMS?

My greatest achievement has been to work with Information System Security Officers (ISSOs) to address and solve complex and critical security challenges that protect patient Protected Health Information (PHI), regulated by the Health Insurance Portability and Accountability Act (HIPAA). I am proud of the work that I have done to help safeguard patient data and ensure its confidentiality, integrity, and availability.

I am particularly proud of the following accomplishments:

- As a Sr. CRA, I am proud to be able to assist Jr. ISSOs in the implementation of security framework such as Risk Management Framework (RMF) and FedRamp security framework designed to significantly improved the protection of CMS systems and patient PHI.
- I worked with ISSOs to implement and deploy CMS new security controls around the transition from ARS

3.1 to ARS 5.1 policy designed to improve system access and data protection.

- I provided technical support to system business owners during their ATO initiatives, helping them to obtain the necessary approvals and clearances to operate their systems on CMS network.
- I have been recognized by my peers and supervisors for my expertise and dedication to protecting patient data.

In addition to my professional achievements, I am also proud of the relationships that I have built with my colleagues. I have formed lifelong friendships with some of the best people I know, and I am grateful for their support and guidance.

I am excited to continue working with CMS as I believe we have a bright and rewarding future ahead. It is my aspiration to continue working in the field of cyber security and making a difference. I believe that everyone has a responsibility to protect their personal information, and I am committed to doing my part to keep patient data safe.

What is it about being a CRA you enjoy the most?

I most enjoy making a difference as a CMS Senior Cyber Risk Advisor (CRA). I believe that cyber security is a critical field that helps protect people's privacy, financial, and health data. It is also a critical part of protecting CMS' infrastructure. As a CRA, I play a vital role in keeping CMS patients' health data and organizational network systems safe from cyber threats.

- I enjoy solving complex problems, the field of cyber security is constantly evolving, and there are always new threats and challenges I face daily. As a Cyber Risk Advisor, I am challenged to think creatively and come up with innovative solutions to protect CMS systems.
- I enjoy working and collaborating with my CRA peers who are cyber security subject matter expert professionals, as well as working with system business owners and stakeholders to develop and implement effective security measures to protect CMS systems, applications, and networks.
- I enjoy the challenge of staying up to date on the latest cyber threats, as you may know, the cyber threat landscape is constantly changing so it is important to stay up to date on the latest threats and vulnerabilities. As a Cyber Risk Advisor, I consider myself to be a lifelong learner and able to quickly adapt to new challenges.

Of course, there are also challenges to being a Cyber Risk Advisor. The work can be stressful, and I have to sometimes deal with long hours and tight deadlines. However, if you are passionate about cyber security and making a difference in the world, then the rewards of being a Cyber Risk Advisor can be very satisfying.

What tip(s) would you like to share with ISSOs who want to become a CRA?

- If you are interested in becoming a Cyber Risk Advisor, I encourage you to learn more about the field and the skills and qualifications that are required. There are many resources available online that can help you get started.
- I also recommend that you get some hands-on experience with cyber security by volunteering or working part-time in a related field. With hard work and dedication, you can achieve your goal of becoming a Cyber Risk Advisor and make a difference in the world.
- Always find a Sr. CRA who would be willing to mentor you and help bring you a long in the field of cyber security. Study the NIST RMF and CSF and FedRAMP frameworks and live on the NIST.gov. NVD.nist.gov, FedRAMP.gov, and CISA websites.

What are some of the challenges you face as a CRA?

As a CMS Senior CRA, one of my biggest challenges is working with difficult business owners and ISSOs who see me as a threat or hindrance to them meeting their deadlines. They may not realize that we are all on the same team and want to do what's right to protect PHI.

- ISSOs are responsible for the security of their respective systems, and business owners are responsible for the overall success of their business units. As a CRA, I am here to help bridge the gap between the two to ensure that everyone is working together to protect PHI.
- I do this by providing clear and concise communication, being flexible and understanding of their constraints, and helping them to understand the importance of security. I also collaborate with them to develop risk mitigation plans that allow them to meet their deadlines while still protecting PHI.
- It is important to remember that CRAs are not here to prevent business system owners and ISSOs from meeting their obligations and achieving their goals. We are here to ensure that everything is implemented according to CMS policy and to protect as best we can against a data breach. By working together, we can achieve our shared goal of protecting PHI and by placing CMS systems in the best possible security posture.

How do you resolve the work differences that may arise between you and your fellow CRAs?

The best I can describe is that of siblings; we argue and fight like any other family siblings, but at the end of the day we don't hold our heated communications to heart and come together as a family to work out our differences. Sometimes mother Shawnte must break us apart and sometimes she just let us fight it out, respectfully Of course (wink wink!). We are friends and enjoy each other and the work that we do is so rewarding to all of us, especially when we come together to solve very difficult and very complex problems and trust me there have been some doozies over my tenure at CMS.

As a Cyber Risk Advisor (CRA) at CMS, Eric supports and advises ISSOs, all system stakeholders, and CMS management on the best practices of the Risk Management Framework (RMF). He also ensures that CMS system security policies are adhered to according to the recommended security standards in ARS 5.1. In addition, he supports his fellow CRA team members whenever needed.

IAM Roles for Service Accounts: An Aid to Enhancing Zero Trust Maturity in AWS Kubernetes Ecosystems

Mackenzie Wartenberger (with contributions from Sean Patnode, Jeff Bond, the batCAVE Zero Trust team, and CMS Zero Trust team)

Granular access controls, adhering to the Zero Trust principle of 'least privilege', are a cornerstone for any robust security program. Zero Trust is a cybersecurity model that mandates verification checks for every user, service account, and device seeking access to resources, irrespective of their location or network origin. Creating and enforcing granular access controls has been complicated for security practitioners for years,

especially when traditional access controls are unavailable. Traditional methods of managing access within the AWS-Kubernetes realm have often been fraught with challenges — from the risks of credential mishandling to the complexities of ensuring consistent access control across dynamic cloud environments. IRSA emerges as a game-changer, especially for DevOps professionals and cloud security teams. By bridging AWS's IAM capabilities with Kubernetes' service accounts, IRSA presents a more secure, scalable, and auditable solution, aligning closely with the principles of Zero Trust.

What Are IAM Roles for Service Accounts: *Decoding the acronym*

IAM Roles for Service Accounts (IRSA) are an AWS feature that enables you to associate IAM Roles with a Kubernetes service account. Kubernetes Pods can then be configured to use IRSA instead of having to distribute AWS credentials to a cluster. This allows workloads running in a Kubernetes cluster to have securely defined access permissions to utilize AWS services.

What Problem is This Solving: A Lack of Granularity for Access

One well-known issue facing Application Development Organizations (ADOs) launching within CMS Cloud is the lack of direct control over Identity Stores and Authentication (AuthN) and Authorization (AuthZ) processes. CMS Cloud-controlled resources protect ADOs from the risk involved in managing all their own identity and access management, however, they also limit ADO's ability to create more granular access rules within their internal environments. While IRSA does not help ADOs manage access for human users or developers, they do offer a solution for NPE access control within proprietary environments, solving potential over-provisioning and permissions sprawl issues.

IRSA's Interplay within AWS and Kubernetes: *A Gateway to Zero Trust Security*

The integration of IRSA within an AWS ecosystem involves intricate interactions between the AWS environment and the Kubernetes ecosystem. IRSA acts as a conduit, allowing Kubernetes pods to seamlessly interface with AWS services while managing data flow traffic within the AWS Virtual Private Cloud (VPC) network. This layered approach between AWS, Kubernetes, and IRSA safeguards against unauthorized lateral movements (micro-segmentation), minimizing the potential attack surface, and introduces an extra point of AuthN and AuthZ for machine-to-machine interactions.

Adding IRSA to the CMS Landscape: Playing Nice with ARS and Zero Trust

We have proved that IRSA helps to enforce least privilege and micro-segmentation, but an additional benefit to implementing IRSA within CMS is its alignment to both the CMS Acceptable Risk Safeguards (ARS) Controls and specific Zero Trust security principles. To put this benefit into context, the CMS Zero Trust Working Group is currently organizing a data call for all HHS ADOs to evaluate Zero Trust Maturity, the results from which will be assessed against the CMS-specific version of the CISA Zero Trust Maturity Model. Within that CMS Zero Trust Maturity Model are numerous "security functions" where the comprehensive use of well-crafted IRSA directly enhances an ADO's Zero Trust Maturity. A final benefit for both CMS ARS Control compliance and Zero Trust Maturity enhancement is the enrichment of log data created by adding IRSA to a network, allowing for improved visibility into, and non-repudiation of, access flow throughout an environment. For a complete cross-reference of the CMS ARS Controls supported by IRSA implementation and how they relate to security controls (as defined by the CISA Zero Trust Maturity Model), please see below:

CMS ARS Control Compliance addressed by IRSA	CMS ZT Maturity Model Functions strengthened by IRSA
AC-02-Account Management	ID-Authentication-NPEs
AC-03-Access Enforcement	ID-Identity Stores APIs
AC-04-Information Flow Enforcement	ID-Access Management
AC-06-Least Privilege	ID-Visibility and Analytics
AC-09-Previous Logon Notification	DE-Resource Access
AC-12-Session Termination	DE-Visibility and Analytics
AU-08-Time Stamps	AW-Application Access Authentication APIs
AU-10-Non Repudiation	AW-Visibility and Analytics
AU-12-Audit Generation	DA-Data Access
CM-05-Access Restrictions for Change	DA-Visibility and Analytics
CM-07-Least Functionality	
CA-09-Internal Systems Connections	
IA-03-Device Identification and Authentication	
SA-15-Development Process, Standards, and Tools	
SC-28-Protection of Information at Rest	

Specifics of IRSA adoption within batCAVE: *Lessons Learned the batCAVE Way*

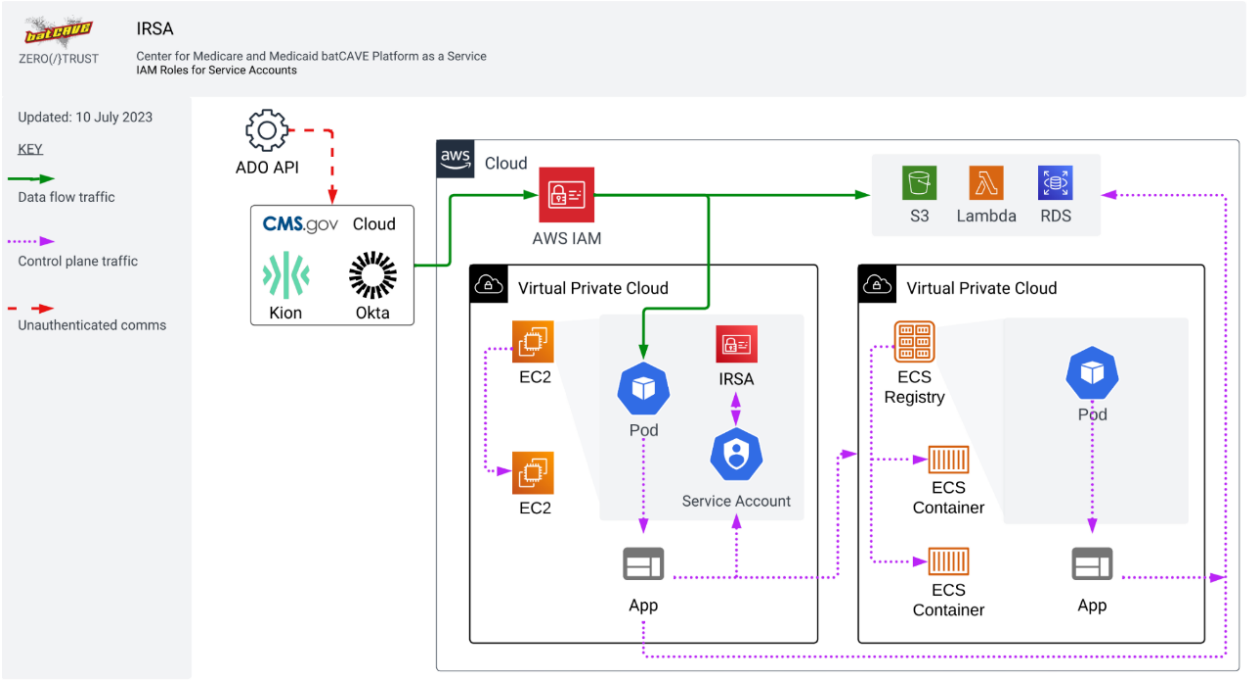
Like other ADOs launching in CMS Cloud, batCAVE (Continuous Authorization and Verification Engine) has limited input over IAM roles and Identity Stores, which are controlled by CMS Cloud–posing a challenge to granular access management. IRSA implementation delivers batCAVE developers and engineers a workaround to define granular permissions/roles for Kubernetes service accounts within the batCAVE ecosystem and associate them with AWS service account roles. IRSA implementation allows AWS and Kubernetes resources to have tightly controlled interactions–a critical component supporting least privilege, micro-segmentation, and a robust Zero Trust security posture. By leveraging IAM Roles for Service Accounts, batCAVE Devs can ensure that the applications running in their Kubernetes clusters have the necessary permissions to interact with AWS services within the AWS Virtual Private Clouds (VPCs) while maintaining a secure, controlled, and auditable data flow environment. Through the process of implementing IRSA in batCAVE, the Zero Trust teams have formulated the following guidelines for realizing the full potential of IRSA and seamlessly embedding it within the zero-trust model:

- **Segregation of Principals:** Limit the ability to perform IAM actions impacting IRSA (creation, modification, or deletion) to system administration roles to limit accidental or malicious manipulation of settings.
- **Precision through Role-based access control (RBAC):** Prioritize the allocation of role-specific permissions when configuring IRSA, ensuring that over-provisioning is avoided and the least access required for specific tasks will be granted.
- **Avoiding Wildcards:** Avoid using wildcards and employ explicit permissions to limit the potential attack surface and blast radius.
- **Continuous Reviews and Audits:** Regularly review and audit IAM policies and access control mechanisms for Service Accounts to maintain alignment with evolving security demands.

Conclusion: Bringing Some Control to What We Can

No security environment can be controlled entirely, but IAM Roles for Service Accounts help support robust Zero Trust Maturity within AWS Kubernetes ecosystems and are a valuable aid for adding control in situations where Access Management is limited. The tactical integration of IRSA into an ecosystem manages machine-to-machine interactions, enables more fine-grained controls for ADOs launching on CMS Cloud, and elevates

overall cybersecurity resilience. As the cybersecurity landscape continues to evolve, IRSA's strategic implementation offers a valuable counterbalance to a dynamic threat landscape.



IRSA Architecture:

High-level architecture illustrating the flow of permissions requests using IRSA. A request is initiated by an ADO API and authenticated via CMS Cloud resources (Kion, Okta). This AuthN would authorize an ADO API to utilize an AWS IAM role contained in the batCAVE AWS Identity Store. Using that AWS IAM role, the ADO API accesses AWS resources (S3, Lambda, RDS) and applicable batCAVE virtual private clouds containing Kubernetes pods. Each Pod has an attached Service Account, redirecting traffic back to the AWS IAM ID store for Service Accounts for another round of AuthN and AuthZ, involving additional rules and policies corresponding to a specific assigned role. Once a pod AuthN's and is AuthZ'ed via the IRSA, they will have granular permissions and access to applications running in K8s clusters on the batCAVE backend - creating verified and more secure control-place traffic for pod-to-app, pod-to-container, pod-to-VPC, and pod-to-AWS communications.

Mack Wartenberger is a Security Architect at Aquia, Inc., supporting batCAVE Zero Trust. An advocate for securing the digital transformation, Mack is passionate about advancing cyber security in the public and private sectors in GRC, Architecture, and Zero Trust.

Assessing Vulnerability Risks with the Exploit Prediction Scoring System (EPSS)

Lloyd Evans

Part 1: EPSS, A History

Proactive vulnerability management is of critical importance in helping organizations identify and address security weaknesses before they can be exploited — reducing the risk of data breaches, downtime, and reputational damage. Assessing, tracking, and remediating vulnerabilities in systems is a responsibility shared by security teams, developer teams, and business owners. Vulnerabilities source from a combination of tooling and assessments like container vulnerability scanning, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Penetration Testing, etc. For this conversation, let's look specifically at Common Vulnerabilities and Exposures (CVEs).

There are numerous methods for managing vulnerabilities. Some rely on more qualitative methods and system context — producing data that is descriptive and conceptual — while others take on a more quantitative approach — producing data that can be counted, measured, and expressed using numerical values. Both methods may assign scoring to vulnerabilities to assist in risk assessment and prioritization practices.

As I'm sure many reading this have experienced, scaling qualitative practices proves quite difficult. While in-depth contextual analysis may be the most effective approach to addressing a vulnerability, system maintainers quickly encounter practical challenges with more complex systems where thousands of vulnerabilities may be present. Not every system has access to (or business justification for) the resources required to take on that workload.

Thankfully, quantitative resources have been developed and iterated on by special interest groups (SIGs) dedicated to helping the security community address these challenges. Two of these SIGs are led by the Forum of Incident Response and Security Teams (FIRST): the Common Vulnerability Scoring System (CVSS) and the Exploit Prediction Scoring System (EPSS). The first, CVSS, ought to be very familiar with security practitioners. CVSS has long been the traditional method used to score and prioritize CVEs. The second, EPSS, is relatively new (with the first release of public scores in January 2021).

The security community has produced many whitepapers, articles, and analyses on the effectiveness and reliability of EPSS (a few which are linked below). For the sake of this article, we'll focus on the tactical uses of EPSS and how this can directly improve your systems security processes.

Let's review the standard definition of risk:

Risk = Likelihood × Impact

Risk, likelihood, and impact are each concepts that can be assessed using various methods, including qualitative assessments (such as expert opinions and qualitative scales) and quantitative data (such as statistical analysis and numerical measurements), to provide a comprehensive understanding of the overall risk landscape.

As expressed in the below image (Figure 1), using CVSS alone provides an incomplete picture of the risk that a given CVE represents. This is expressed explicitly by FIRST in their CVSS documentation: "CVSS is designed to measure the severity of a vulnerability and should not be used alone to assess risk." This isn't to say that CVSS should not be used, this is to say that CVSS provides a useful but incomplete look into the severity of a CVE

(severity being a component of impact).

This brings us to EPSS.

EPSS provides part of our missing context. As stated in the EPSS documentation, EPSS scoring communicates "the probability of observing any exploitation attempts against a vulnerability in the next 30 days." To clarify, this refers to the probability of observing any exploitation attempts against a vulnerability on some system in the wild. Used in combination with CVSS and KEV, EPSS now allows us to view the risk of a vulnerability through the lens of complementary quantitative data sources.

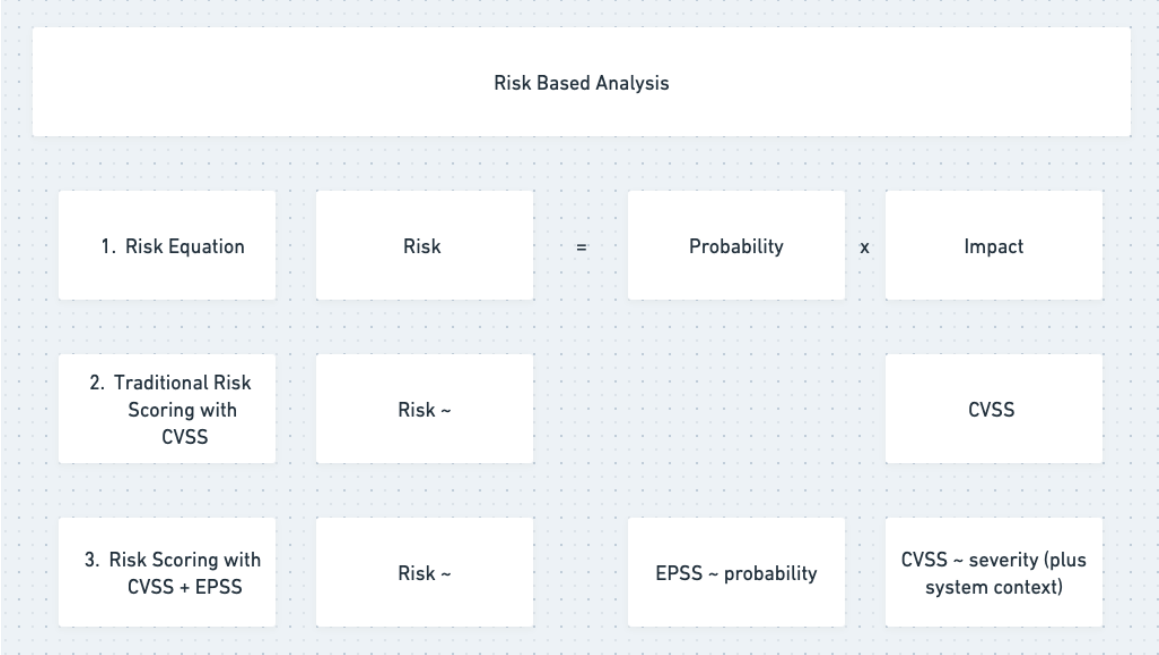


Figure 1. Risk-Based Analysis

This analysis is simplified to address the point, however, there are nuances to take into account. EPSS relates specifically to the "Threat" component of their risk formula and does not, by itself, represent a fully comprehensive assessment of risk.

Until that fully comprehensive data-driven scoring system is created, using the data-driven systems we currently have available allows us to more effectively assess and prioritize CVEs and spend our limited security resources on the highest leverage activities.

Part 2: EPSS in Practice

Let's look at a practical example of EPSS in use with an example application.

If we look at Figure 2, a select output of CVEs from a Grype Container Vulnerability scan of the intentionally vulnerable application "Juice Shop," two 9.8 vulnerabilities stand out that would traditionally be "highest priority critical vulnerabilities" that we'd need to focus our immediate attention on. Using EPSS, however, we can also now see that the first has a score of .01045 and the second has a score of .00083.

That's a 1% and .08% chance of exploitation in the next 30 days.

You'll see that there's also a 7.4 CVSS vulnerability that also has a 1% chance of exploitation in the next 30 days.

Using CVSS alone, that vulnerability wouldn't be addressed before the 9.8 with a .08% chance. Using CVSS alone, each of the >9 CVSS vulnerabilities would be treated unequivocally as critical and a "top priority" for remediation, triggering the immediate expense of security and engineering dollars to remediate.

App	CVE ID	Description	CVSS Score	EPSS Score
juice-shop	CVE-2019-10744	Prototype Pollution	9.1	0.01552
juice-shop	CVE-2023-29017	Potential Remote code execution	9.8	0.01045
juice-shop	CVE-2020-8203	Prototype Pollution	7.4	0.01036
juice-shop	CVE-2023-30547	Exception sanitization vulnerability	9.8	0.00083

Figure 2. Juice Shop CVE Example

I do want to reiterate that these are still vulnerabilities found in the system and it is not my intention to downplay that by any means. That being said, research has shown that the vast majority of CVEs are below a 1% chance of exploitation. Using EPSS, we have access to an additional data set where we can contextualize lower CVSS-scored vulnerabilities that have a high chance of exploitation as well as higher CVSS-scored vulnerabilities that have a low chance of exploitation.

How does this play out in the context of your application?

Let's say an ISSO is tasked with a risk-based decision of a 7.4 CVSS-scored vulnerability that can't be engineered around without significant effort from the engineering teams. The 7.4 CVSS score by itself might (correctly) indicate caution in accepting this risk. This ISSO, however, uses EPSS in addition to CVSS and sees there is a 1% chance that the vulnerability may be exploited in the next 30 days. This analysis gives the ISSO confidence to accept the risk and document their rationale as part of the risk-based decision.

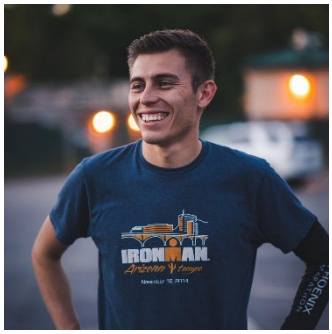
Another ISSO for a large system recently received a vulnerability report with 3,000 CVEs and is up against an assessment deadline to triage and remediate these findings. They only have enough time to remediate the most critical vulnerabilities. Instead of solely using CVSS and wading through contextual analysis of hundreds of critically CVSS-scored vulnerabilities, the ISSO runs a script to update the report with EPSS in addition to CVSS. The ISSO sees that 95% of the 3,000 vulnerabilities have an EPSS score below .01 (1% chance of exploitation). The remaining 150 vulnerabilities above .01 EPSS are a diverse assortment of low, medium, high, and critical CVSS-scored vulnerabilities (an analysis that would not get done in time going through each CVE line by line). The application team is able to remediate each of these top 150 vulnerabilities and contextualize the remaining ones in the backlog for remediation after their assessment.
Now, what if the EPSS score changes?

EPSS regularly updates and tunes its scoring methodology as new information comes out. With regular scanning, an ISSO can view what vulnerabilities are above a threshold that they deem too high of a risk (1%, 5%, 25%, etc.) and prioritize those for remediation using CVSS as supplemental information. If there's a 4.3 CVSS

vulnerability that now has an 87% chance of exploitation, shouldn't that be prioritized above the 9.8 with .08%? These are questions the ISSO is now better equipped to address with data informing their decision process.

Conclusion

EPSS (in the same camp as CVSS) unfortunately doesn't apply to all risks that can be found within a system, but for the vulnerabilities it does apply to, it provides a great deal more context to properly inform risk-based decisions and prioritize vulnerabilities that pose a risk to our systems. By focusing on the vulnerabilities that present the highest risks to our system, we cut down inefficiencies and improve system security posture while optimizing the cost of security and development hours.



Lloyd Evans currently serves as the Principal ISSO and Security Automation Tech Lead for the batCAVE within CMS. Lloyd is the Director of Governance, Risk, and Compliance at Aquia and an Air Force Veteran with experience in the federal ecosystem spanning the Air Force, U.S. Navy, and the United States Department of Health and Human Services (HHS).

Resources:
https://www.csoonline.com/article/644203/how-epss-3-0-is-an-improvement-over-previous-versions-of-the-threat-assessment-system.html
https://www.first.org/epss/faq
https://blog.stackaware.com/p/deep-dive-into-the-epss

What are the chances?

A follow-on to "Assessing Vulnerability Risks with EPSS" by Lloyd Evans and Casey Douglas, CCSQ ISSO

Have you ever checked the chances of winning the lottery? If not, the people who don't buy the tickets will always tell you exactly what the odds are - slim. Why play when the odds are stacked against you? The answer is because there is a "chance" that it might happen. You might win. There's a bigger chance that you'll lose. That's how probability works. There's enough data on the players and winners collected over time to predict the chance that you'll win. It's up to you to decide if you're willing to play or not.

We take chances every day. I took a chance by attending ISPG Demo Day to see if there was something interesting going on over there. Lloyd Evans was demonstrating how batCAVE was using the Exploit Prediction Scoring System (EPSS). Right then, I felt like I just won on a $20 scratch-off. Here's why.

I've been around when Snyk was first turned on for a few systems. Snyk stands for "**S**o **n**ow **y**ou **k**now" and in those moments we wished we hadn't found out – the sentiment that "everyone's Snyk looks like that" didn't make me feel better. I've seen some systems that had hundreds of vulnerabilities. Vulnerabilities that never showed up in other tools. Developers have been saying for a long time that some vulnerabilities are just noise. I heard them, didn't want to hear it, and also didn't want to ignore it.

Remediation prioritization is often determined by first seeking out the Cybersecurity & infrastructure Security

Agency (CISA) Known Exploited Vulnerabilities (KEV) and sorting other vulnerabilities by the CVSS severity category (i.e., critical, high, medium, low). It goes a little something like this: remediating "critical" and "high" vulnerabilities within the timeframes established (15, 30 days, Binding Operational Directive (BOD)19-02); and then, remediating "medium" and "low" (90, 365 days). It sounds like it would make sense. In practice, it's a different story altogether.

CVSS is currently the only source we're using for remediation priority. It's limited in the ability to assess the actual threat that it poses. It doesn't claim to be the anything other than what it's for – measuring the severity of a vulnerability. Yes, you can go beyond the CVSS Base score with added temporal and environmental metrics and do a risk analysis to determine the actual risk. In reality, we use the CVSS score given to us- usually it is the Base score. There are too many vulnerabilities to give each one special treatment.

With the count of published vulnerabilities increasing year after year, some teams manage to collect a decent size backlog. This backlog mostly consists of "medium" and "low" findings. I mention "medium" and "low" because remediation timeframes are greater and the idea that these severity levels are not as big of a deal as "critical" and "high", these get pushed off until later. The problem is that attackers don't care about the listed CVSS severity category. CISA has noticed that some of the bigger attacks have included vulnerabilities rated as "medium", or even "low".

Product teams do their best to manage the vulnerability backlog by setting aside time and resources to chip away at the backlog but not sure if we are spending time investigating and remediating the ones that really matter – the ones that will be exploited. The reality is, according to CISA, less than 4% of vulnerabilities are actually exploited.

EPSS enters the scene. **NOTE:** I won't go into detail about it. I hope you've read Lloyd's article on "Assessing Vulnerability Risks with EPSS" before reading this.

I wanted to try it out. The idea is that we should go from using one data source (CVSS) to using multiple data sources (CVSS, EPSS) when determining remediation priority. Many vulnerability management tools are embracing EPSS. A Security Engineer on one of our teams, Andrew Lee (Bellese), and I talked about it and decided to give it a go. AWS Inspector had EPSS built in already, so we were able to experiment. We were sold. We told all of our friends about it and started sharing out additional resources such as https://www.first.org/epss/api , https://github.com/Hoplite-Consulting/EPSS-CLI; to get them in on the action.

For now, we're limited on how we can use EPSS since we're held to the remediation timeframes that are based on CVSS severity category. If we're lucky, that'll change soon to include EPSS probability scores. That doesn't mean we aren't going to use EPSS where we can. Say you observed a "medium" vulnerability with a 70% probability of being exploited in the next 30 days. Would you take your sweet time since you're given 90 days to remediate? That's a chance I wouldn't take.

Postscript: At the time that we experimented with EPSS, Snyk did not have it available. Snyk is starting to move towards a new risk-based model for their Open Source and Container products, leveraging information like EPSS and reachability to help prioritize and reduce noise.
https://snyk.io/blog/improved-risk-assessment-with-epss-scores-in-snyk/
https://snyk.io/blog/introducing-new-risk-score/

If you're interested in exploring this in a test Snyk Org for your CMS project, contact Mike Kania on CMS Slack or email michael.kania@cms.hhs.gov to get set up to test it out. Any questions or feedback can also be dropped into the #snyk_security channel on CMS Slack.

Casey Douglas is an ISSO working for CCSQ/ISG/IS3

Data Minimization and Minimum Necessary Collections in CMS Systems

Jake Moldowsky

In the past quarter, the Privacy office has received many inquiries surrounding the collection of expanded or new datasets of Personally Identifiable Information (PII). To help foster a larger CMS discussion about when a data collection activity may be appropriate, OIT Privacy is publishing this refresher around the agency's obligation of data minimization. The goal of this article is to equip the reader with a foundational set of questions to help strike a balance between the use of personal data at CMS and the risk of exposure from overly broad data practices.

Background:

In 2021 the Biden Administration signed Executive Order 13985, mandating that federal agencies take concrete steps to advance equity in their programs. Under this order, CMS must "allocate resources to address the historic failure to invest sufficiently, justly, and equally in underserved communities, as well as individuals from those communities." As reiterated in 2023, "Each agency head shall support ongoing implementation of a comprehensive equity strategy that uses the agency's policy… data-collection processes … and regulatory functions to yield equitable outcomes for all Americans, including underserved communities." [1]

To make headway on implementation at CMS, many programs have begun to collect data on a more granular level than originally proposed. Some examples are related to income, race, ethnicity, sexual orientation, gender orientation, or in many cases information related to a specific outreach activity (e.g., beneficiary phone number, income variables, or survey responses). When increased collections are specifically tailored to defined program results, they can offer immense insights for remedying past inequities or paving the way for the agency's future. However, in many instances there are legal and ethical considerations to the scope of records the government should maintain in CMS Systems of Record. Below, I elaborate on some relevant standard-of-practice considerations:

Fair Information Practice Principles (FIPPS)

Rooted in a 1973 Federal Government report from the Department of Health, Education, and Welfare Advisory Committee, "Records, Computers and the Rights of Citizens," the Fair Information Practice principles (FIPPS) have informed many Federal statutes, the laws of many U.S. states, and have been incorporated into the

[1] Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government, (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/)

policies of organizations around the world.[2]

All CMS IT Systems should be measured against the FIPPS in an iterative process from inception to retirement. We could discuss each of the FIPPs for hours, but today we will focus on one specific principle:

Data Minimization

Any data collection proposed by a CMS program should be intentional and "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed". Now, before you go and delete all data fields stored in your systems, data minimization does not in operation mean to strip program resources bare; rather, through a collaborative process between your program and the Privacy Office, data collected, used, and disclosed will be justified against the purpose for which the collection supports.

Here are some ways you can ensure that your system is only collecting the minimum necessary and proportionate data prior to implementing the activity, saving your program resources and frustrations:

- Proactively create a document outlining your collection proposal written with a high level of specificity and its defined purpose and outcome.
    - Include exactly which data elements are critical to your work.
    - Include a justification and crosswalk for how each specific element will concretely contribute to a goal.
- Talk to your technical team, ISSO, and CRA to understand the limits and scope of your activity.
    - Understand from what source your data will be collected, with a strong preference towards directly from the subject individual.
    - Are you standing-up a new system? Is this activity a modification to an existing collection? Will that require an update to your Privacy Impact Assessment (PIA)?

The Privacy Act of 1974 and System of Record Notices (SORNs)

All PII collected or maintained at CMS must coordinate with a SORN written description for that activity.[3] Additionally CMS cannot collect data that is not described in the "Categories of Records" section, of a SORN, nor disclose PII except subject to one of twelve exceptions[4] in the Privacy Act, or as written as a "Routine Use" in the SORN text. In addition to a permissible pathway, the Privacy Act includes instructions to federal agencies around how to use PII:

Relevant and Necessary[5]

> "Maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."

[2] These include Access and Amendment, Accountability, Authority, Minimization, Quality and Integrity, Individual Participation, Purpose Specification and Use Limitation, Security and Transparency. For more information on the origin of the FIPPS, please visit this Federal Privacy Counsel Resource

[3] CMS SORNs can be found here

[4] Department of Justice Guidance on the Privacy Act of 1974

[5] 5 U.S.C. § 552a(e)(1)

Where should you get data from if there are multiple potential sources?[6]

> "Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs."

The Privacy Office most often helps advise on these principles when existing collections are expanded beyond their SORN description under "Categories of Records Collected". Additionally, when data is collected for a certain purpose, it may not be shared across CMS for an alternative purpose than written in the SORN. In any instance, if there is ambiguity on whether your proposed activity is described by a SORN, or if you need assistance locating the correct SORN for your system[7], please reach out to our office at the contact below.

Conclusion

Questions around data minimization will likely become more common in CMS' work as the agency incorporates Artificial Intelligence (AI) and increasingly needs to facilitate bias testing, or as divisions seek to purchase commercial data and grapple with how to share data as "One CMS".

If you have any questions about the above or seek to discuss how to best work within your business needs to comply with the many requirements around data collection, please reach out to the privacy team at Privacy@cms.hhs.gov.

Jake Moldowsky is a Senior Privacy Analyst for ECS Federal, supporting OIT privacy working across CMS programs. In addition to operating the CMS privacy mailbox, Jake advises on questions of US privacy law, incident risk management, and system privacy-by design.

What is Vishing and how to protect yourself against it?

Saad Zulqadar

Vishing, also known as "voice phishing", is a type of social engineering attack that preys on human psychology and trust. Cybercriminals use phone calls to impersonate legitimate entities such as banks, government agencies, or even tech support services. They employ various tactics to manipulate recipients into divulging confidential information, such as credit card numbers, Social Security numbers, passwords, and more.

Common Vishing Techniques

Caller ID Spoofing: Cybercriminals often manipulate caller ID information to appear as a trusted entity, increasing the likelihood of the victim answering the call.

[6] 5 U.S.C. § 552a(e)(2)

[7] There is often, but not always, a 1-to-1 relationship between IT Systems and Systems of Record

Urgency and Fear: Attackers create a sense of urgency or fear, claiming that the recipient's account has been compromised, taxes are owed, or legal action will be taken if immediate action isn't taken.

Empathy and Personalization: Vishing attackers may use personal information, obtained through previous data breaches or online searches, to establish credibility and empathy, making the victim more likely to comply.

Protecting Yourself Against Vishing

Verify the Caller: Always verify the authenticity of the caller before sharing any personal information. Call back the official number of the organization from their official website or a trusted source.

Avoid Sharing Sensitive Information: Legitimate organizations will not ask for sensitive information over the phone, such as passwords or PINs. Be cautious about sharing any such information.

Report Suspicious Calls: If you receive a suspicious call, report it to the appropriate authorities or the organization being impersonated. This helps prevent further attacks and protects others from falling victim.

Upcoming CFACTS Training

Saad Zulqadar

The next *Working with CFACTS – Introduction to Risk Management & RMF training* will take place September 12th -13th. This is a virtual training session that will be held for two days from 9:00am-4:00pm ET. This is an introduction course designed for new ISSOs and CRAs, or junior level ISSOs new to the CMS Cybersecurity program.

The course targets the NIST Risk Management Framework (RMF) based around the NIST Special Publication 800-37 (Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy).

The course will use the CMS FISMA Continuous Tracking System (CFACTS) to map the steps within the RMF to some basic workflows in the CFACTS tool.

Sign up today if you are interested by contacting the ISPG training team at CMSISPGTrainers@cms.hhs.gov.

2023 Cyberworks Event

Saad Zulqadar

CMS is hosting a special event during October, which is Cybersecurity Awareness Month! Cybersecurity professionals like you can showcase their projects to gain industry recognition and make meaningful connections with the CMS cybersecurity community. This year's Cyberworks event will take place on October 25th and will run from 9:00am-12:30pm. The event will cover topics such as:

- Enabling multi-factor authentication
- Using strong passwords

- Keeping your computer updated
- Recognizing and reporting phishing

Add the event to your calendar: Add to Calendar
You can join the event by using the following link: 2023 Cyberworks Event Link.
If you have any questions, please contact the ISPG training team at CMSISPGTrainers@cms.hhs.gov.

Saad Zulqadar is with Premier and supports the ISPG Cybersecurity Workforce Support and Training Team.

Cybersecurity Community Forum Notes from June, July, and August 2023

Cole Schenck (Assyst)

In June 2023:

- Chelsea Delestathis presented to us ISPG Demo Days, live demonstrations to give CMS staff and contractors awareness of ISPG's products, solutions, architecture, services, and tooling which took place in June.
- Teresa Proctor gave a presentation about Security Data Lake (SDL), a centralized repository designed to store, process, maintain secure, and govern large amounts of data relevant to an organization's security posture. She explained the benefits, the mission, the objectives, updates, and the priorities of SDL.
- Joshua Meagher gave us a demonstration of the new computer-based training (CBT) upgrade leaning management system. He showed off the new user interface and all the cool features they added to CBT to make for a better experience for CMS employees and contractors.

In July 2023:

- Elizabeth Schweinsberg informed everyone of an upcoming HHS Zero Trust Data Call. She informed us that the HHS requested CMS to collect information about Zero Trust from each FISMA system. The request is 40 questions that takes about 1-2 hours to complete.
- Leslie Nettles gave a presentation about contract language requirements and the contract attestation process. She gave us a background about information security and walked us through the information technology procurements document, required deliverables to support information security and privacy

requirements, and the contractor attestation process.

- Joan Michelle Yi gave us a step-by-step demo on how to complete a security and risk assessment request on the Signal application.

In August 2023:

- Desmond Young educated us about the importance of keeping data in CFACTS up to date. He gave examples of how data in CFACTS is used at CMS, what types of information is missing in CFACTS, what data is missing in POA&Ms, and pointed us to the CFACTS artifacts page to help us with updating missing information.
- Leslie Nettles gave a call to action for CMS employees and contractors. To improve security and confidentiality of CMS information systems, she requests that we review and categorize current CMS information types per NIST 800-60 vol 2 guidelines.
- Elizabeth Schweinsberg gave us a friendly reminder of the HHS Zero Trust data call like the one in July. The request is 40 questions and can be completed in 1-2 hours.

The C3F PowerPoint slides and recordings can be found on C3F Confluence Page.

Cole Schenck works with Assyst within ISPG on the ISSO Advocacy and Support Program (IASP).

CISAB Notes from June, July, and August 2023

Cole Schenck, (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 June meeting, Casey Douglas and Derek Bailey wanted the cohort's input about the levels of encryption being used during Zoom cloud meetings. After some discussion, the cohort determined that there needs to be more clarity about whether PII/PHI can be discussed in Zoom chats. Derek Bailey was curious what the cohort thought about CMS's new phishing campaign. More specifically, what were other ISSOs and Data Guardians' reaction to it. Don Bartley explained to the cohort the purpose of the campaign and the methods used to educate those who clicked on the phishing emails during the campaign. Cohort members shared their

experience with previous phishing campaigns and offered suggestions for future ones. An anonymous CISAB member wanted to know what the cohort thought about downloading CMS information on personal computers. They also wanted to know what the Contractor Data Use Agreement (DUA) allows them to do with CMS information on their personal computer. The cohort had a fruitful conversation about the inconsistencies in contract language regarding storing CMS information on personal computers.

In our July meeting, Derek Bailey wanted to hear from the cohort if they thought their systems would be a good fit for OA or if it would cause headaches. Jason King explained to the cohort how OA's function and the requirements systems need to meet to opt into them. Derek Bailey wanted to get some feedback from cohort members how they're finding Signal to be. Derek Bailey, LAaron Johnson, and Andrew Moorshead provided feedback and discussed the pain points they're facing using Signal and possible remediations. Don Bartley and Cole Schenck wanted to hear from the cohort if they thought it would be a better idea to change the ISSO Journal into a blog format on the cms.security.gov website. The cohort agreed it would be better for the Journal to remain as is when it moves to the cms.security.gov website.

In our August meeting, Derek Bailey wanted to know more about technical outputs and what it meant to each assessment team. However, Derek was unable to attend this meeting, so we were unable to get more context. An anonymous cohort member asked the cohort about compliance remediation timeframes. Rob shared with us that EPSS calculations are being implemented into vulnerability reporting to assist with assessments. Zil Zukhruf Sheikh wanted to share a video demonstration for ISSOs filing a M-21-31 login questionnaire on CFACTS as well as a video demonstration of the ACT Review Team reviewing a M-21-31 login questionnaire on CFACTS.

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 September CISAB meeting will be held September 27th at 11AM. We look forward to seeing you there!

Cole Schenck works with Assyst within ISPG on the ISSO Advocacy and Support Program (IASP). He acts as secretariat for the CISAB group.

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

ISPG Training Calendar at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ISPG-Training-Catalog.pdf

CMS Information Security Library at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

NIST Cybersecurity Framework at https://www.nist.gov/cyberframework

NICE Cybersecurity Workforce Framework at https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

US-CERT at https://www.us-cert.gov/

SANS at https://www.sans.org/

OWASP at https://www.owasp.org/index.php/Main_Page