CMS ISSO Journal

...by and for CMS Cybersecurity Professionals

October-December 2023

Issue 26

CMS ISSO JOURNAL

October-December 2023 Issue 26

Highlights

Welcome to the fourth 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.

- Curious how ISSOs can leverage AI to their advantage in the ever-evolving digital landscape? Find out more in **Safeguarding the Digital Frontier: The Role of Information System Security Officers in the AI-Powered Cybersecurity Era**
- Interested in phishing-resistant multifactor authentication? **Phishing-Resistant MFA: A Critical Need in 2024** has you covered
- Not sure what the Security Data Lake has been up to recently? Read **What's Going on With the Security Data Lake (SDL)? A Self-guided FAW With the Latest Information Available for Cyber Risk Management Stakeholders at CMS** to find out the details.
- 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

ISSO Bootcamp Pilot Kickoff Coming In 2024! 6

What is an Information System Security Officer (ISSO)? 6

What is the ISSO Bootcamp? 7

Goals of the ISSO Bootcamp 8

Selected IBC Training is compliant with CMS ISSO NICE Framework Roles and KSA's 8

Safeguarding the Digital Frontier: The Role of Information System Security Officers in the AI-Powered Cybersecurity Era 11

The Evolving Landscape of Cybersecurity 11

Introduction to the Role of Information System Security Officers (ISSOs) 11

The Increasing Importance of Integrating AI in Cybersecurity 12

The Evolving Role of ISSOs 12

Traditional Responsibilities of ISSOs in Securing Information Systems 12

Challenges Faced by ISSOs in the Rapidly Changing Cybersecurity Landscape 12

The Need for ISSOs to Adapt and Embrace Technological Advancements 13

Definition of AI and Its Broad Applications 13

The Intersection of AI and Cybersecurity 13

The Potential Benefits of Incorporating AI into Security Practices 14

ISSOs Embracing AI in Cybersecurity 14

Recognition of the Changing Threat Landscape 14

The Role of ISSOs in Adopting AI-Driven Tools and Solutions 15

How AI Enhances the Efficiency and Effectiveness of Cybersecurity Efforts 15

AI Applications in Cybersecurity 16

Addressing Challenges in AI Integration into Cybersecurity 18

Looking to the Future: AI's Growing Role in Cybersecurity 19

The Growing Importance of AI in the Cybersecurity Landscape 19

Continuous Adaptation and Learning for ISSOs 19

Emerging Trends and Technologies in AI and Cybersecurity 19

Embracing the Future 20

Conclusion: Empowering the Future of Cybersecurity with ISSOs and AI 20

Recap of the Evolving Role of ISSOs 20

The Transformative Impact of AI on Cybersecurity 20

The Crucial Role of ISSOs in Securing Digital Landscapes with AI 20

ISPG will transition away from the Risk Management Handbook 21

What is changing? 21

Why is this change happening? 22

What can I expect moving forward? 22

Enhancing Security: The Intersection of Threat Modeling and Implementing Zero Trust Principles 23

Introduction 23

Understanding Threat Modeling... 23

Zero Trust Principles Overview 23

Integrating Threat Modeling into Zero Trust Design 23

Conclusion 24

New features and big changes on the ISPG website 25

ISPG News & Updates blog is live 25

The Information Security & Privacy Library is being retired 26

Some templates are now on CyberGeek 26

SaaSG Adoption of the Rapid Cloud Review (RCR) Policy in CMS IS2P2 27

Phishing-Resistant MFA: A Critical Need in 2024 30

Multi-Factor Authentication: A Primer for Phishing-Resistant Concepts 30

Popular MFA Methods in the Era of Smart Devices 31

Understanding User Vulnerability: The Case of Evilginx 32

The FIDO Alliance: Pioneering Enhanced Authentication Standards 33

Securing the Future: Implementing FIDO2 and Phishing-Resistant MFA in 2024 34

Be on the Lookout for Those Phishing Traps! 35

Welcome to a New Way of Learning all Things Cybersecurity 35

ISSO – Exploring the Next Frontier 36

Supply Chain Risk Management (SCRM) at CMS and Across the United States Federal Government. 38

Wait, I Needed That: Criticality Analysis 43

What's Going on With the Security Data Lake (SDL)? A Self-guided FAQ With the Latest Information Available for Cyber Risk Management Stakeholders at CMS 45

What will this article tell me about the SDL? 45

Can you remind me what the SDL is and why I should care? 45

Ok, when can I expect to see these changes? 46

How long is the transition period? 46

Have more questions? Reach out to the team! 46

Cybersecurity Community Forum Notes from September, October, and November 2023 47

CISAB Notes from September and November 2023 48

Internal and External Resources for ISSOs 49

Confluence Sites 49
Web 49

ISSO Bootcamp Pilot Kickoff Coming In 2024!

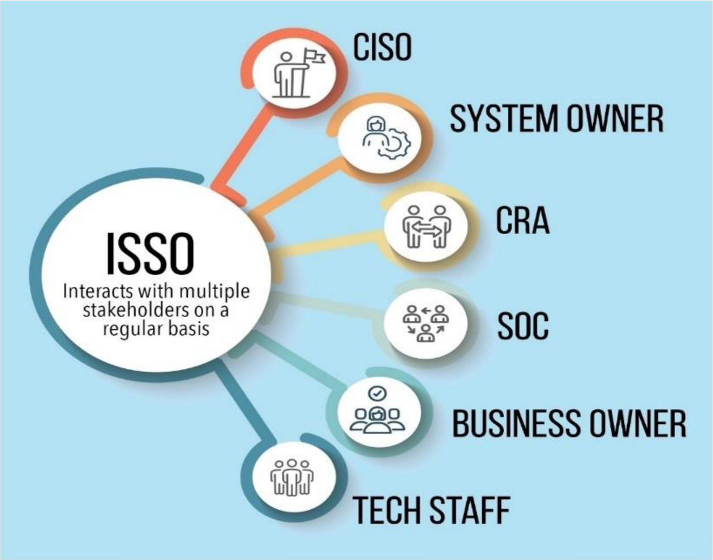
Curtis Criswell, MBA, CISSP, HCISPP

You're a new ISSO.... now what?
Prepare yourself for success,
Get started with the ISSO Boot Camp.
BOOT CAMP
ISSO BOOT CAMP
Email ISSO@CMS.HHS.GOV for more information

What is an Information System Security Officer (ISSO)?

An ISSO serves as the principal advisor to the Information System Owner (SO), Business Process Owner (BO), Chief Information Security Officer (CISO), and liaises with the Cyber Risk Advisor (CRA) on all matters, technical and otherwise, involving the security of an information system. ISSOs are responsible for ensuring the implementation and maintenance of security controls in accordance with the Security Plan (SP) and Department of HHS and CMS policies. Typically, ISSOs will be called on to provide guidance, oversight, expertise, development of security documents and the implementation of security controls. While ISSOs may not actually perform all functions, they will have to coordinate, facilitate, or otherwise ensure certain activities are being performed. As a result, it is important for ISSOs to build relationships with the SO, technical staff, and other stakeholders.

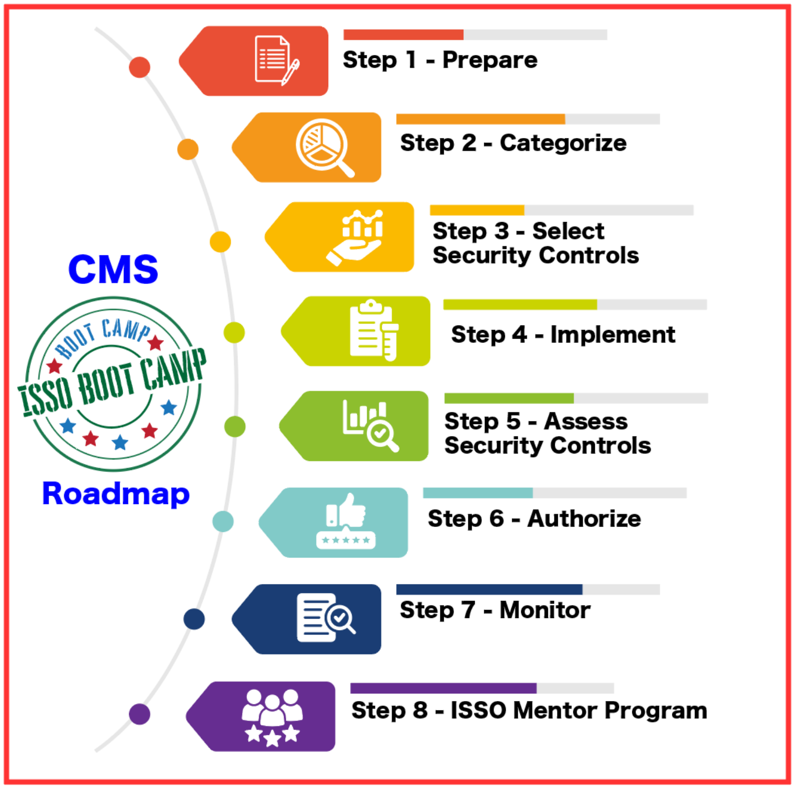
ISSO's are in a unique position that they must interact with varied stakeholders on a regular basis. An example of the array of personnel whom ISSOs interact with:



What is the ISSO Bootcamp?

Because of the critical role and responsibilities of the ISSO to the overall risk and security posture of CMS; the Cybersecurity Workforce Support and Training Program (CWSTP) ISSO Advocacy and Support Program (IASP) has sponsored the ISSO Boot Camp (IBC) initiative. The role of an ISSO is critical for ensuring security and privacy compliance for FISMA systems, this initiative dedicated to helping ISSOs succeed improves the overall security posture and culture at CMS.

The IBC is an initiative that has curated training classes tailored to progress the skillset of an ISSO from no matter where their ISSO skills proficiency level is currently. For ISSOs to provide adequate security support for their assigned systems, a solid educational background in information security is needed. This training will compliment not replace what is currently provided by the Information Security and Privacy Group (ISPG). The goal is to bring all ISSOs to a common CMS centric security skillset starting from a non-CMS centric security perspective. The training will align with the CMS ISSO duties of executing the CMS centric Risk Management Framework process.



The following security training topics are addressed:

• Application Security	• Disaster Recovery Management	• Network Security
• Risk/Vulnerability Management	• Security and Policy Training	• Privacy
• Security Assessments	• Host Environments (cloud, etc.)	• Incident/Breach Planning and Response
• Mandated Compliance	• FISMA/FedRAMP Compliance	• Security Operations (including Continuous Monitoring)

Goals of the ISSO Bootcamp

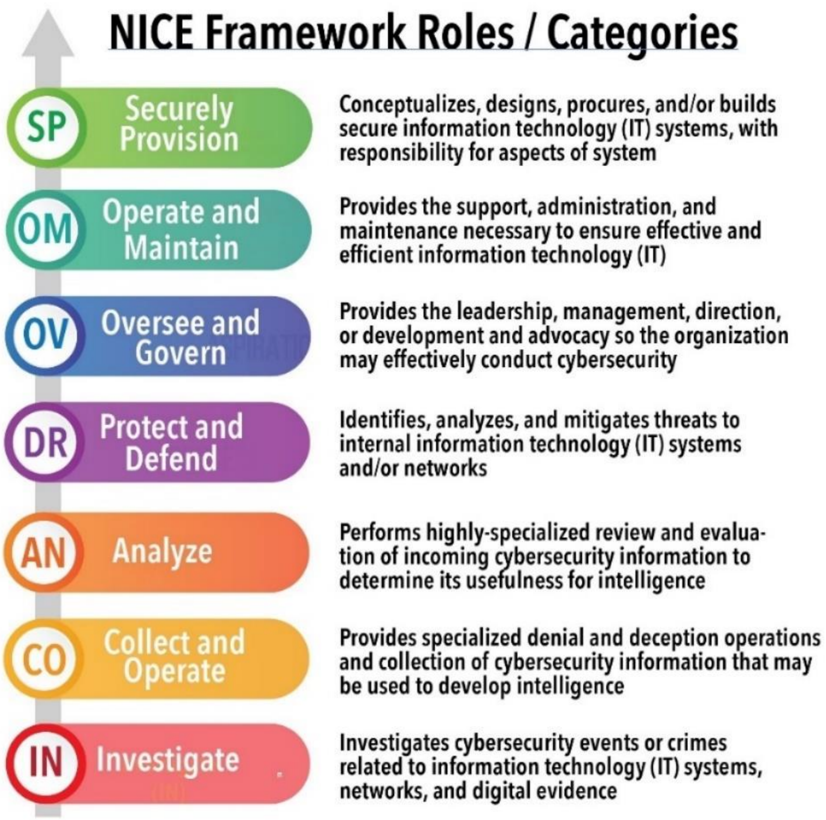
- Helping ISSOs succeed in their roles as CMS professionals.
- Objectives include leveling ISSOs' security and privacy knowledge and sharing a better understanding of CMS security and privacy standards.
- Developing a core set of security training requirements and cross walking to existing courses, establishing a core set of ISPG-offered training courses.
- Formalize the ISSO Position to revolve around developing the ISSO from a collateral "duties as assigned" role to an acknowledged CMS formal position, and developing a job progression and career path
- Identifying and tracking completion of training opportunities for ISSOs who are more senior and have an advanced proficiency level skillset.
- Develop a mentoring program for ISSOs who are looking for professional peer collaboration.
- Establishing regular two-way communications methods with ISSOs.

Upon completion of the IBC, the ISSO should be considered a "Fully Capable" CMS ISSO functioning at the moderate proficiency level.

- A "Fully Capable ISSO" is an individual who has the required Knowledge, Skills, Ability (KAS's), training and experience to successfully accomplish the duties and responsibilities of an ISSO as defined in the CMS Information Systems Security and Privacy Policy.
  - The ISSO must have extensive knowledge of basic concepts and processes as well as experience applying these with only periodic high-level guidance.
  - The ISSO must be able to perform successfully in non-routine and sometimes complicated situations.
  - The ISSO can draw conclusions and make recommendations.

Selected IBC Training is compliant with CMS ISSO NICE Framework Roles and KSA's

Knowledge, Skills, and Abilities (KSAs) are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training.



NICE Framework Roles / Categories

SP Securely Provision: Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system

OM Operate and Maintain: Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT)

OV Oversee and Govern: Provides the leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity

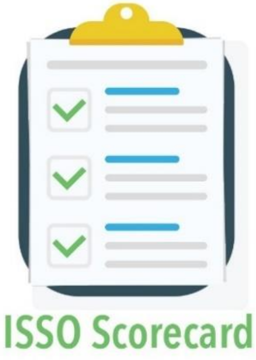
DR Protect and Defend: Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks

AN Analyze: Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence

CO Collect and Operate: Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence

IN Investigate: Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence

Note: see link for more in detail on the NICE Framework Categories, Roles, and KSA's
National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (nist.gov)
As an ISSO, your NICE code is OV-MGT-001. Knowing this will help you find additional appropriate training for tasks or knowledge areas.



The ISSO Scorecard is a tool that is currently being utilized to assist with determining an ISSO's proficiency level based upon demonstrable prior experience and ISSO Scorecard Results. The ISSO will start the IBC training from the corresponding level of Scorecard results and proficiency level. The ISSO Scorecard and IBC are designed to promote Entry level ISSO's to Intermediate and solidify and strengthen skills of existing Intermediate ISSOs. The ISSO Scorecard will be regularly revised to maintain relevance to changing policies, mandates, emerging technologies, and processes.

The ISSO Toolkit contains links to documents a CMS ISSO will access often in their daily activities, and resources to support their work. CMS ISSOs should become familiar with the purpose and usage of each. *The Information Security and Privacy Group (ISPG) provides the "CyberGeek" website as a one-stop shop for all security and privacy related information at CMS – including dedicated resource pages for ISSOs and other roles*. This is a new site, and more information will become available as it grows.

Go to ISPG website (CyberGeek)

- **Documents** (selected examples)
    - HHS Information System Security and Privacy Policy (IS2P)
    - CMS Acceptable Risk Safeguards (ARS 5.0)
    - CMS Information Security and Privacy Policy (IS2P2
    - CMS Risk Management Handbooks (RMH)

- **Tools and Resources** (selected examples)
    - CFACTS
    - CMS Target Life Cycle (TLC)
    - ISSO Framework
    - CMS ISSO Journal
    - CMS Slack - List of Slack channels that will help on your journey to becoming a fully capable ISSO:
        - #ars-feedback
        - #cfacts_community
        - #cisab
        - #cms-isso
        - #cyber-risk-management
        - #ispg-all
        - #isso-as-a-service
        - #security_community

- **ISSO Mentorship Program -** The CMS ISSO Mentorship Program seeks to improve the overall readiness and skill of Information System Security Officers (ISSOs) at CMS by creating opportunities for knowledge sharing and support among ISSOs of all experience levels. Both mentors and mentees benefit from a partnership that is structured enough to provide growth towards defined goals – yet flexible enough that anyone can participate.

In conclusion, the IBC is designed to build, strengthen, standardize, and advance the ISSO practice and community at CMS. ARE YOU IN?

Would you like to be a participant of the CMS ISSO Boot Camp Pilot?
Please send us an email - ISSO@cms.hhs.gov

Curtis Criswell, MBA, CISSP, HCISPP
As a Sr. ISSO Lead at CMS, Curtis is currently engaged in the effort to build, strengthen, standardize, and advance the CMS ISSO Community of Practice via targeted training development.

Safeguarding the Digital Frontier: The Role of Information System Security Officers in the AI-Powered Cybersecurity Era

Dr. Mary – Margaret Chantre

In the contemporary era, Artificial Intelligence (AI) has become an integral part of our daily lives, permeating various aspects and industries. From automating mundane tasks to revolutionizing how we interact with technology, AI's influence is ubiquitous. One of the pivotal domains where AI is making substantial strides is cybersecurity. As digital landscapes evolve and threats become more sophisticated, the role of Information System Security Officers (ISSOs) has gained paramount significance. This article explores the dynamic integration of AI in the cybersecurity landscape, shedding light on how ISSOs are at the forefront of this transformative journey.

The Evolving Landscape of Cybersecurity

The digital realm is constantly evolving, presenting both opportunities and challenges. With the increasing reliance on digital infrastructure, the threat landscape has expanded exponentially. Cybersecurity has become a critical concern for individuals, organizations, and governments worldwide. The conventional methods of securing information systems are proving insufficient in the face of advanced and persistent cyber threats. In this ever-changing landscape, the role of ISSOs is pivotal in ensuring the confidentiality, integrity, and availability of sensitive data.

Introduction to the Role of Information System Security Officers (ISSOs)

ISSOs play a crucial role in safeguarding information systems against cyber threats. They are the guardians of digital fortresses, responsible for designing, implementing, and managing security policies and protocols. Traditionally, ISSOs have been tasked with protecting systems from unauthorized access, ensuring compliance with regulations, and responding to security incidents. However, the evolving threat landscape necessitates a paradigm shift in their approach, and AI emerges as a powerful ally in this endeavor.

The Increasing Importance of Integrating AI in Cybersecurity

As cyber threats become more sophisticated, the need for intelligent, adaptive, and proactive cybersecurity measures has never been greater. This is where the integration of AI comes into play. AI brings a new dimension to cybersecurity by leveraging machine learning, natural language processing, and other advanced techniques to analyze vast amounts of data, identify patterns, and detect anomalies in real-time. The ability of AI to learn from historical data and adapt to emerging threats makes it a formidable tool for enhancing the overall cybersecurity posture.

In the subsequent sections, we will delve deeper into how ISSOs are embracing AI in various facets of their roles, from threat detection and prevention to incident response and forensics, access control, authentication, and authorization, and vulnerability management. The synergistic relationship between ISSOs and AI is paving the way for a more resilient and adaptive cybersecurity landscape.

The Evolving Role of ISSOs

Traditional Responsibilities of ISSOs in Securing Information Systems

Information System Security Officers (ISSOs) have long been the stalwarts of digital defense, entrusted with the critical task of safeguarding information systems. Traditionally, their responsibilities have encompassed a range of crucial duties, including:

1. **Access Control:** ISSOs are responsible for implementing and managing access control mechanisms, ensuring that only authorized individuals have the appropriate level of access to sensitive information.
2. **Policy Development:** Crafting and enforcing security policies to establish guidelines for secure system operation and data protection.
3. **Incident Response:** Rapidly responding to and mitigating security incidents, ranging from unauthorized access attempts to data breaches.
4. **Regulatory Compliance:** Ensuring that information systems comply with relevant regulations and standards, safeguarding against legal and regulatory repercussions.
5. **Security Audits:** Conducting regular security audits and assessments to identify vulnerabilities and weaknesses in the system.

Challenges Faced by ISSOs in the Rapidly Changing Cybersecurity Landscape

The cybersecurity landscape is dynamic, marked by incessant technological advancements and an escalating array of cyber threats. ISSOs confront several challenges in adapting to this rapidly changing environment:

1. **Sophisticated Cyber Threats:** The nature of cyber threats is evolving, becoming more sophisticated and elusive. ISSOs must grapple with advanced tactics employed by cybercriminals.
2. **Skills Gap:** The demand for cybersecurity professionals has surged, leading to a skills gap. ISSOs face the challenge of acquiring and retaining skilled personnel.

3. **Technological Complexity:** The integration of new technologies introduces complexity. ISSOs must navigate intricate systems, ensuring they remain secure and resilient.

4. **Regulatory Changes:** The regulatory landscape is dynamic, with laws and compliance requirements frequently changing. ISSOs need to stay abreast of these changes to ensure ongoing compliance.

5. **Insider Threats:** The risk of insider threats, whether intentional or unintentional, poses a significant challenge. ISSOs must implement measures to mitigate these risks without hindering legitimate operations.

The Need for ISSOs to Adapt and Embrace Technological Advancements

In the face of these challenges, ISSOs are compelled to adapt and embrace technological advancements to fortify their cybersecurity strategies:

1. **Integration of Artificial Intelligence:** Embracing AI in threat detection, incident response, and vulnerability management empowers ISSOs to tackle advanced threats with greater efficiency.

2. **Continuous Learning:** ISSOs must engage in continuous learning to stay abreast of emerging threats and evolving technologies. Professional development and certifications play a pivotal role in enhancing their expertise.

3. **Collaboration and Information Sharing:** Establishing robust networks for collaboration and information sharing within the cybersecurity community enables ISSOs to glean insights and best practices.

4. **Automation of Routine Tasks:** Automation of routine security tasks allows ISSOs to focus on more complex aspects of cybersecurity, improving overall operational efficiency.

5. **Strategic Planning:** ISSOs need to engage in strategic planning, aligning cybersecurity efforts with organizational goals and risk tolerance. This involves a proactive approach to risk management.

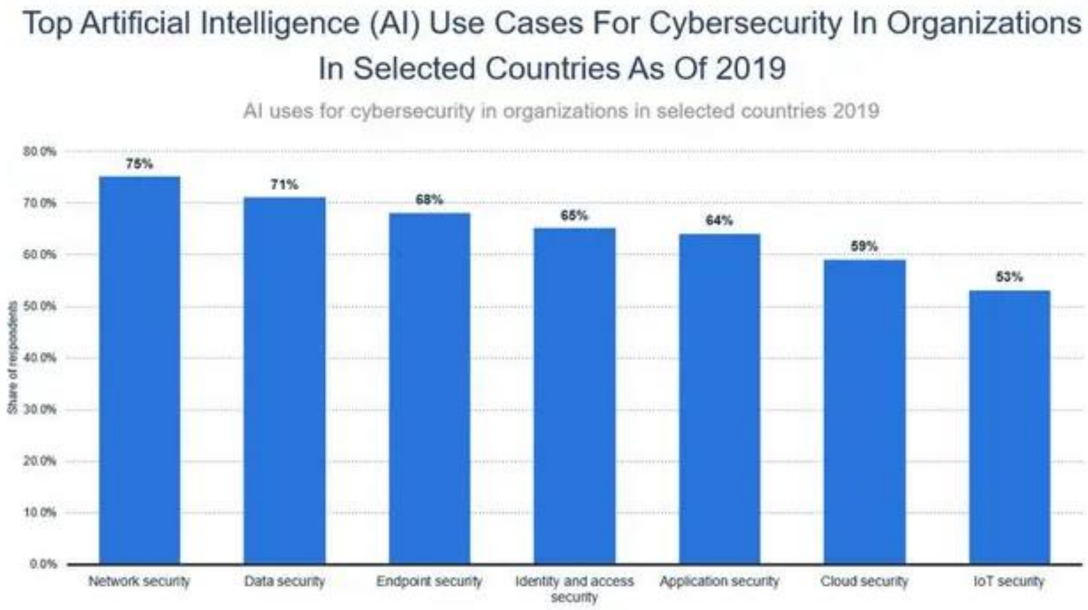
In the subsequent sections, we will explore how ISSOs are leveraging technological advancements, particularly the integration of AI, to overcome these challenges and redefine their role in the ever-evolving landscape of cybersecurity.

Definition of AI and Its Broad Applications

Artificial Intelligence (AI) refers to the development of computer systems capable of performing tasks that typically require human intelligence. These tasks include problem-solving, learning, speech recognition, and decision-making. AI is not limited to a specific application but spans a broad spectrum of uses, ranging from virtual assistants like Siri and Alexa to complex machine learning algorithms powering recommendation systems and autonomous vehicles.

The Intersection of AI and Cybersecurity

In recent years, the intersection of AI and cybersecurity has become a focal point in the ongoing battle against cyber threats. AI technologies, particularly machine learning and deep learning, are increasingly integrated into cybersecurity practices to bolster defense mechanisms. The synergy between AI and cybersecurity offers a proactive approach to identifying and mitigating security risks.



Top Artificial Intelligence (AI) Use Cases For Cybersecurity In Organizations In Selected Countries As Of 2019

AI uses for cybersecurity in organizations in selected countries 2019

Note: Australia, France, Germany, India, Italy, Netherlands, Spain, Sweden, United Kingdom, United States; 2019; 850 Respondents; senior IT executives from IT information security, cybersecurity, and IT operations
Source(s): Capgemini; Statista

The Potential Benefits of Incorporating AI into Security Practices

Incorporating AI into security practices holds immense potential for enhancing the overall cybersecurity posture. Some key benefits include:

1. **Advanced Threat Detection:** AI-powered systems can analyze vast amounts of data, identify patterns, and detect anomalies indicative of potential threats. This enables ISSOs to stay ahead of sophisticated cyber-attacks.

2. **Automated Incident Response:** AI-driven tools facilitate automated incident response, allowing ISSOs to respond swiftly to security incidents. This reduces response times and minimizes the impact of cyber threats.

3. **Efficient Vulnerability Management:** AI enhances vulnerability management by automating the scanning and prioritization of vulnerabilities. This ensures that ISSOs can address the most critical security flaws promptly.

4. **Adaptive Security Measures:** Machine learning algorithms enable systems to adapt to evolving cyber threats. ISSOs can deploy dynamic security measures that adjust in real-time based on the changing threat landscape.

ISSOs Embracing AI in Cybersecurity

Recognition of the Changing Threat Landscape

ISSOs play a pivotal role in recognizing the evolving nature of cyber threats. The traditional approaches to cybersecurity are no longer sufficient against sophisticated and rapidly mutating threats. Recognizing this shift, ISSOs are increasingly turning to AI-driven tools to fortify their defenses.

The Role of ISSOs in Adopting AI-Driven Tools and Solutions

ISSOs are at the forefront of adopting AI-driven tools and solutions as part of their cybersecurity arsenal. This involves:

1. **Strategic Integration:** ISSOs strategically integrate AI tools into existing cybersecurity frameworks, ensuring seamless collaboration between human expertise and AI capabilities.
2. **Tool Evaluation:** ISSOs meticulously evaluate AI-driven cybersecurity tools, considering factors such as accuracy, scalability, and the ability to integrate with existing systems.
3. **Training and Skill Development:** ISSOs invest in training and skill development to harness the full potential of AI technologies. This involves staying informed about the latest advancements and best practices in AI-driven cybersecurity.

How AI Enhances the Efficiency and Effectiveness of Cybersecurity Efforts

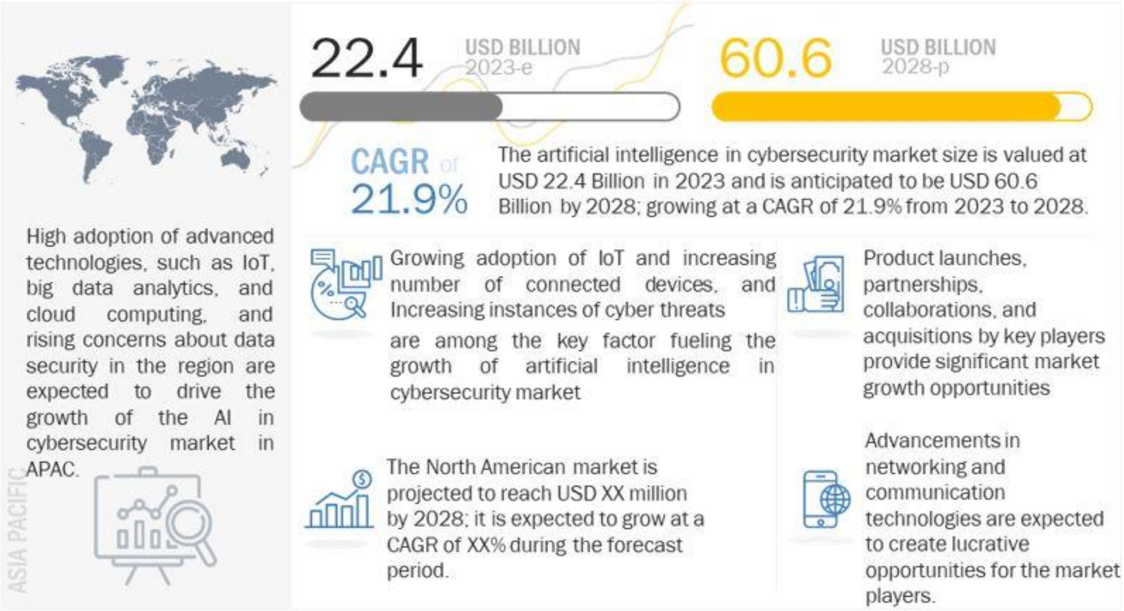
The incorporation of AI into cybersecurity practices brings about a paradigm shift in terms of efficiency and effectiveness:

1. **Proactive Threat Mitigation:** AI enables proactive threat mitigation by identifying patterns and anomalies that precede an actual attack. This proactive stance is crucial in preventing security breaches before they occur.
2. **Rapid Incident Response:** AI automates incident response processes, enabling ISSOs to respond rapidly to security incidents. This not only reduces response times but also minimizes the impact of cyber threats on organizational operations.
3. **Continuous Learning and Adaptation:** Machine learning algorithms continuously learn from new data, adapting to emerging threats. This dynamic adaptation ensures that cybersecurity measures remain effective in the face of evolving attack techniques.

In the subsequent sections, we will delve deeper into specific use cases where ISSOs are leveraging AI to address the challenges posed by the dynamic cybersecurity landscape.

AI Applications in Cybersecurity

As Information System Security Officers (ISSOs) navigate the complex and evolving landscape of cybersecurity, the integration of Artificial Intelligence (AI) applications becomes instrumental. Let's explore how AI is applied across key domains within cybersecurity:



The artificial intelligence in cybersecurity market size is valued at USD 22.4 Billion in 2023 and is anticipated to be USD 60.6 Billion by 2028; growing at a CAGR of 21.9% from 2023 to 2028.

High adoption of advanced technologies, such as IoT, big data analytics, and cloud computing, and rising concerns about data security in the region are expected to drive the growth of the AI in cybersecurity market in APAC.

Growing adoption of IoT and increasing number of connected devices, and Increasing instances of cyber threats are among the key factor fueling the growth of artificial intelligence in cybersecurity market

Product launches, partnerships, collaborations, and acquisitions by key players provide significant market growth opportunities

The North American market is projected to reach USD XX million by 2028; it is expected to grow at a CAGR of XX% during the forecast period.

Advancements in networking and communication technologies are expected to create lucrative opportunities for the market players.

1. Threat Detection and Prevention

AI-powered Intrusion Detection Systems (IDS)

ISSOs leverage AI-powered IDS to monitor network traffic and system logs. These systems learn normal network behavior, identifying anomalies that may signify unauthorized access attempts or malicious activities. Machine learning models adapt to evolving attack techniques, enhancing detection accuracy.

Malware Detection with AI Algorithms

AI algorithms play a crucial role in identifying and mitigating malware threats. By analyzing file characteristics, behavior, and code patterns, AI aids in classifying potential malware variants based on malicious intent. Continuous learning from new samples enables AI to adapt to emerging malware trends.

Anomaly Detection Using AI-based Techniques

AI-based anomaly detection techniques identify unusual activities or deviations from standard patterns in network traffic, system logs, or user behavior. Learning from historical data, AI establishes baselines and raises alerts when deviations occur, indicating potential security incidents or attacks.

2. Incident Response and Forensics (IR/F)

Automated Incident Response through AI

AI automates specific incident response activities, including initial triage, data collection, and containment. ISSOs employ AI-powered systems to autonomously respond to alerts, analyze relevant data, and make informed decisions swiftly, reducing response times in high-alert environments.

Security Analytics and Forensics with AI

AI enhances security analytics and forensic investigations by rapidly analyzing large volumes of data, logs, and digital artifacts. Machine learning algorithms identify patterns, extract relevant information, and correlate events to reconstruct attack scenarios. AI assists in identifying indicators of compromise (IoCs) and attributing attacks.

Proactive Threat Hunting with AI Capabilities

ISSOs use AI for proactive threat hunting, leveraging its capabilities to analyze data and identify potential threats before they escalate. AI-driven threat hunting involves continuous monitoring, pattern recognition, and analysis of indicators that may signify impending security issues.

3. Access Control, Authentication, and Authorization (AC/A/A)

Behavioral Biometrics and AI

AI analyzes and models user behavioral patterns, such as keystrokes and mouse movements, for continuous user authentication. Behavioral biometrics strengthen access control by creating unique user profiles, helping identify potential account compromises or insider threats.

Anomaly Detection for Access Control

ISSOs implement AI algorithms for anomaly detection in user behavior, triggering additional authentication measures or raising alerts for potential unauthorized access attempts. AI enhances access control systems by identifying and responding to deviations from standard user activity.

Strengthening Authentication through AI

AI contributes to strengthening authentication mechanisms by incorporating adaptive authentication methods. ISSOs deploy AI-driven solutions to assess and authenticate users based on evolving patterns and risk factors, enhancing overall access security.

4. Vulnerability Management (VM)

AI in Vulnerability Scanning and Patch Management

AI automates vulnerability scanning and patch management by analyzing system configurations, software versions, and patch levels. Machine learning models identify known vulnerabilities and prioritize patch deployment based on risk scores, impact assessments, and exploit likelihood.

Predictive Analytics for Vulnerability Assessment

AI leverages historical vulnerability data, threat intelligence feeds, and system telemetry for predictive analytics in vulnerability assessment. By analyzing patterns and correlating information, AI algorithms identify potential attack vectors and provide proactive recommendations for vulnerability mitigation.

Balancing Automation and Human Oversight in VM

ISSOs strike a balance between automation and human oversight in vulnerability management. While AI streamlines processes, human expertise remains essential for interpreting results, validating findings, and making informed decisions in complex cybersecurity scenarios.

In the subsequent sections, we will delve into specific use cases and examples illustrating how ISSOs effectively integrate these AI applications to address cybersecurity challenges and fortify organizational defenses.

Addressing Challenges in AI Integration into Cybersecurity

The integration of Artificial Intelligence (AI) into cybersecurity brings about transformative advancements, but it also introduces a set of challenges that Information System Security Officers (ISSOs) must address. Let's explore these challenges and the corresponding strategies to overcome them:

1. Potential Challenges in Integrating AI into Cybersecurity

Rapid Technological Evolution

As AI evolves, ISSOs face the challenge of keeping pace with rapid technological advancements. Continuous updates, new AI-driven tools, and emerging threat vectors require ISSOs to stay vigilant and adapt their cybersecurity strategies accordingly.

Legal and Regulatory Compliance

The use of AI in cybersecurity raises questions about compliance with international laws and regulations. ISSOs must navigate legal complexities, ensuring that AI applications adhere to data protection laws, privacy regulations, and industry-specific compliance standards.

2. Adversarial Attacks on AI Systems and Countermeasures

Vulnerability to Adversarial Attacks

AI systems are susceptible to adversarial attacks, where threat actors manipulate input data to deceive AI algorithms. ISSOs must anticipate and mitigate adversarial attacks that aim to exploit vulnerabilities in AI-powered security solutions.

Countermeasures for Adversarial Attacks

Implementing robust countermeasures is crucial for defending AI systems against adversarial attacks. ISSOs can deploy techniques such as adversarial training, where AI models are trained with adversarial examples to enhance their resilience against manipulation.

3. Ensuring Transparency and Explainability in AI Algorithms

Lack of Transparency in AI Decisions

AI algorithms often lack transparency, making it challenging to understand the reasoning behind their decisions. This lack of transparency raises concerns about accountability, trust, and the ability to verify the accuracy and fairness of AI-powered security systems.

Strategies for Ensuring Transparency

ISSOs can address the transparency challenge by advocating for the development of explainable AI (XAI) techniques. XAI methods provide insights into how AI algorithms reach specific decisions, enhancing transparency and enabling stakeholders to comprehend the rationale behind AI-driven cybersecurity measures.

Looking to the Future: AI's Growing Role in Cybersecurity

As we stand at the intersection of artificial intelligence (AI) and cybersecurity, it's evident that the future holds even greater significance for Information System Security Officers (ISSOs). Let's explore the evolving landscape and the imperative for ISSOs to adapt and embrace emerging trends in AI and cybersecurity.

The Growing Importance of AI in the Cybersecurity Landscape

AI's influence on cybersecurity has transcended novelty, becoming an indispensable force in defending against evolving threats. The symbiotic relationship between AI and cybersecurity is poised to deepen, with AI becoming not just a tool but a strategic ally in the battle against cyber adversaries. ISSOs must recognize and harness the growing importance of AI to fortify their defense mechanisms.

Continuous Adaptation and Learning for ISSOs

In the dynamic realm of cybersecurity, adaptation is not just a virtue but a necessity. ISSOs face the ongoing challenge of staying abreast of AI advancements, threat landscapes, and regulatory changes. Continuous learning and professional development are imperative for ISSOs to effectively integrate AI into their security strategies and preemptively counter emerging cyber threats.

Emerging Trends and Technologies in AI and Cybersecurity

AI-Powered Threat Intelligence

The future holds a surge in AI-powered threat intelligence, enabling ISSOs to proactively identify and respond to threats. Machine learning algorithms will sift through massive datasets, uncovering subtle patterns indicative of potential threats and providing real-time insights to bolster cyber defenses.

Autonomous Security Operations

AI-driven autonomous security operations are on the horizon, revolutionizing how ISSOs manage and respond to incidents. Automated incident response, powered by AI algorithms, will streamline decision-making processes, significantly reducing response times and mitigating the impact of cyber incidents.

Quantum Computing and AI

The convergence of quantum computing and AI presents both opportunities and challenges. ISSOs must prepare for the transformative impact of quantum computing on cryptographic protocols, necessitating the development of quantum-resistant AI algorithms to secure sensitive information in the quantum era.

Embracing the Future

In conclusion, the future demands a symbiotic relationship between ISSOs and AI, characterized by a proactive stance, continuous learning, and adaptability. As AI cements its role in cybersecurity, ISSOs must navigate the evolving landscape with foresight, leveraging emerging trends and technologies to fortify their organizations against cyber threats.

The journey ahead involves not just embracing AI as a technological tool but fostering a cybersecurity ecosystem where AI is an integrated, intelligent partner. ISSOs, as guardians of information systems, play a pivotal role in shaping this future, ensuring a resilient defense against the ever-evolving challenges in the cybersecurity landscape.

Conclusion: Empowering the Future of Cybersecurity with ISSOs and AI

In retrospect, the journey through the evolving landscape of Information System Security Officers (ISSOs) and the transformative integration of Artificial Intelligence (AI) in cybersecurity paints a vivid picture of the dynamic nature of our digital defenses.

Recap of the Evolving Role of ISSOs

ISSOs have long been the guardians of digital fortresses, entrusted with securing information systems against an ever-expanding array of cyber threats. Traditionally tasked with roles encompassing threat detection, incident response, access control, and vulnerability management, ISSOs have weathered the changing tides of technology and adversarial ingenuity.

However, in the face of an increasingly sophisticated threat landscape, ISSOs have had to adapt. The role has evolved from conventional responsibilities to embracing technological advancements, with a pivotal shift toward incorporating AI into the cybersecurity arsenal.

The Transformative Impact of AI on Cybersecurity

The infusion of AI into cybersecurity represents a paradigm shift, empowering defenders with intelligent tools capable of learning, adapting, and predicting. AI-driven threat detection, automated incident response, behavioral biometrics, and predictive analytics have redefined the efficacy of cybersecurity measures.

ISSOs, once reliant on traditional methods, now leverage AI to navigate the intricate web of cyber threats. This transformative impact transcends routine tasks, offering a proactive defense mechanism that augments human capabilities and outpaces the speed of evolving threats.

The Crucial Role of ISSOs in Securing Digital Landscapes with AI

As sentinels of the digital realm, ISSOs stand at the forefront of the AI revolution in cybersecurity. Their crucial role extends beyond conventional responsibilities to actively embracing AI-driven tools and solutions. ISSOs are not mere overseers; they are orchestrators of a harmonious symphony where human expertise collaborates seamlessly with AI intelligence.

In securing digital landscapes, ISSOs wield AI as a force multiplier, enhancing the efficiency and effectiveness of cybersecurity efforts. The future demands a holistic approach where ISSOs navigate the complexities of AI integration, address challenges, and continually adapt to emerging trends.

In this dynamic landscape, ISSOs emerge as architects of resilience, steering organizations toward a future where AI fortifies cybersecurity defenses. The transformative journey signifies not just a technological evolution but a strategic alliance between human insight and artificial intelligence, ensuring a robust defense against the ever-evolving threats in the digital age. As we embrace this synergy, ISSOs play a pivotal role in empowering the future of cybersecurity, where AI becomes an intelligent ally in the perpetual quest for digital resilience.

Dr. Mary Margaret Chantre. I am the Program Manager for the CyberVets Program at Premier Enterprise Solutions. The CyberVets program helps veterans transition into the civilian life and aids in getting jobs in the Cybersecurity field.

ISPG will transition away from the Risk Management Handbook

ISPG Policy Team

What you need to know about this change and how it will impact your daily work

The debut of CyberGeek has allowed ISPG to re-evaluate the way we publish and manage our core documents. CyberGeek is now the official ISPG website and serves as the single source of truth for security and privacy at CMS.

The new website aims to provide:

- Policy guidance in plain language that is digestible and easy to understand
- Clear text that breaks down complex compliance activities into actionable content and next steps
- An improved experience for content publishers, who can now make changes and edits without having to rely on versioned PDFs

As more new content becomes available, ISPG leadership is also looking at some of our legacy documents and seeing where we can make improvements – including the Risk Management Handbook (RMH).

What is changing?

With the launch of CyberGeek, you may have noticed that the current chapters of the RMH can be found on a page called CMS Security and Privacy Handbooks. This page will be the new home for all updated policy Handbooks produced and maintained by ISPG.

The CMS Security and Privacy Handbooks are designed to be helpful resources that guide the activities of CMS staff and contractors who support the development, operations, maintenance, and disposal of CMS information systems. They are aligned with the NIST SP 800-53 catalog of security controls, which are the foundation for CMS's security and privacy standards. The Handbooks also support the risk management approach laid out in the NIST Risk Management Framework and the Federal Information Security Management Act (FISMA).

Over time, the RMH chapters will be modified and absorbed into the broader CMS Security and Privacy Handbooks for a more flexible approach to procedural guidance – not dependent on specific security controls, but still covering all the topics needed to help CMS staff and contractors follow policies, standards, and best practices.

Why is this change happening?

CMS has made many changes in an effort to evolve the processes and procedures we use to keep systems and user data safe. Programs like Ongoing Authorization (OA), Adaptive Capabilities Testing (ACT), and Continuous Diagnostics and Mitigation (CDM) are moving CMS towards a compliance approach that is:

- Risk-driven rather than compliance-driven
- Capability-oriented rather than control-oriented
- More understandable and actionable

The decision to move away from control-based documentation and instead focus on system capabilities was made to better-align CMS policies with current NIST standards. This directly impacts documents like the RMH, which was structured tightly around controls.

What can I expect moving forward?

As we implement this change, you can expect to see more Handbooks focused on system capabilities rather than specific controls. That means – for example – that instead of using the former *RMH Chapter 1: Access Control (AC)*, you will find on CyberGeek the new CMS Access Control Handbook.

Stay tuned to CyberGeek for more information and new Handbooks coming soon! As always, if you have questions about security and privacy policy and how it impacts your system, reach out to the experts on Slack at **#ispg-sec_privacy-policy,** who can help you get the answers you need.

Enhancing Security: The Intersection of Threat Modeling and Implementing Zero Trust Principles

Maril Vernon (Aquia)

Introduction

As Zero Trust continues to gain momentum within the security community, organizations strive to properly identify and implement its pillars. One tool that is often overlooked as an aid to validating Zero Trust is threat modeling. Threat modeling helps identify and prioritize potential risks, while Zero Trust principles provide a framework for implementing strong security controls over multiple layers. In this article, we will explore the intersection of threat modeling and implementing Zero Trust principles, highlighting how these two practices can work together to enhance security and mitigate emerging threats.

Understanding Threat Modeling

Threat modeling is a method of proactive security that involves identifying potential threats, analyzing their potential impact, and determining effective countermeasures. It helps organizations gain a comprehensive understanding of their attack surface, vulnerabilities, and potential adversaries. Threat modeling can be performed at various levels, such as application, network, or system-wide, to identify potential weaknesses and develop appropriate security measures.

Zero Trust Principles Overview

Zero Trust is a security approach that challenges the traditional perimeter-based security model “trust but verify.” It operates on the principle of "never trust, always verify," assuming that no user or device is inherently trustworthy. In a practical sense this means not trusting who a user is because they have authenticated to a system before. Each request, source, and destination is validated, every single time. Zero Trust principles advocate for strong authentication, continuous monitoring, and strict access controls to minimize the risk of unauthorized access and lateral movement within the network. This approach helps organizations establish granular control and visibility over their assets.

Integrating Threat Modeling into Zero Trust Design

Threat modeling plays a crucial role in the design and implementation of Zero Trust architectures. By incorporating threat modeling into the process, organizations can identify potential threats and vulnerabilities specific to their environment. This information enables them to tailor their Zero Trust implementations to address the most significant risks effectively.

1. Identifying Potential Threat Scenarios:

   Threat modeling helps organizations identify potential threat scenarios and attack vectors. By considering various threat scenarios, such as external attacks, insider threats, or supply chain risks, organizations can develop a more robust and comprehensive Zero Trust architecture. Threat modeling ensures that the Zero Trust implementation is not only focused on known threats but also considers emerging and evolving risks.

2. Prioritizing Security Controls:

   Threat modeling provides insights into the potential impact and likelihood of different threat scenarios. This information helps organizations prioritize security controls and allocate resources effectively. By aligning threat modeling findings with the Zero Trust principles, organizations can implement appropriate access controls, authentication mechanisms, and monitoring capabilities where they are needed the most.

3. Continuous Iteration and Improvement:

   Both threat modeling and Zero Trust principles require a mindset of continuous iteration and improvement. Threat modeling should be an ongoing process, regularly reevaluating risks and incorporating new information. Similarly, Zero Trust implementations should be continually fine-tuned and adapted to address emerging threats and changing organizational needs. The iterative nature of both practices ensures that security measures remain effective over time.

4. Collaborative Approach:

   The intersection of threat modeling and Zero Trust implementation requires collaboration between security teams, architects, and relevant stakeholders. Threat modeling involves input from various departments and subject matter experts, ensuring a holistic understanding of potential risks. Similarly, implementing Zero Trust principles involves close coordination between security teams, network administrators, and system owners to align access controls and verification mechanisms.

Conclusion

The intersection of threat modeling and implementing Zero Trust principles provides a powerful combined approach to enhancing security against system-relevant threats. By incorporating threat modeling into Zero Trust design, organizations can identify and prioritize potential risks, ensuring that security controls are implemented where they are most needed. This collaborative and iterative approach strengthens the overall security posture, enabling organizations to mitigate emerging threats and protect their critical assets effectively. By embracing the synergy between threat modeling and Zero Trust principles, organizations can establish a strong foundation for a resilient and adaptive security framework.

Learn more about Threat Modeling at CMS:

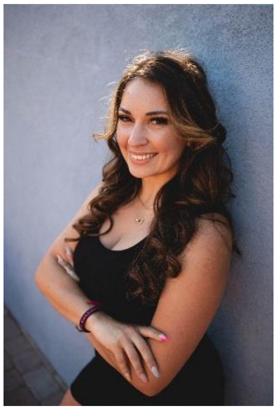
1. Check out the CMS Threat Modeling page on ISPG CyberGeek: https://security.cms.gov/learn/threat-modeling
or
CMS Threat Modeling page on ISPG Confluence (training, videos, etc.): https://confluenceent.cms.gov/display/CTM/

2. Join the #cms-threat-modeling channel on CMS Slack.

3. Email the 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

CASP Threat Modeling Team - Robert Hurlbut, Maril Vernon, Eric Rippetoe
CASP Lead - Eric Rippetoe
CMS / ISPG Contacts: Michael Kania, Robert Wood



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

New features and big changes on the ISPG website

Meg Murray

We hope you've had an opportunity to check out the new home for the **CMS Information Security and Privacy Group (ISPG)** located at security.cms.gov. This project, lovingly referred to as CyberGeek, is your one-stop for the latest information about the policies, programs, and tools managed by ISPG. The site was designed to:

- Point people to the resources and information they need to accomplish their tasks
- Provide information that is current, authoritative, and easy to understand
- Replace and expand upon the former CMS Information Security and Privacy Library
- Offer the latest cybersecurity news, updates, and events at CMS

Since the site launched in June 2023, the CyberGeek Team has worked to develop new site features and we've received lots of helpful feedback from users. As a result, we've been able to iterate on content and make meaningful changes that reflect users' needs. We wanted to tell you about the exciting new features and changes on CyberGeek today.

ISPG News & Updates blog is live

CyberGeek was created to be the home for all the latest cybersecurity and privacy news and events at ISPG. We're excited to announce that the CyberGeek News and Updates blog is live on the site! On the blog, you can:

- See the latest updates from your favorite ISPG Teams including the Policy Team, Front Office, and the Training and Awareness Team
- Get information about important policy changes that impact your daily work
- See event recaps from popular events you may have missed like the C3 Forum and CyberWorks

There's new content being created all the time, so bookmark https://security.cms.gov/posts and check back often! The CyberGeek Team is also investigating ways to deliver a content digest directly to your email, so stay tuned for more updates.

The Information Security & Privacy Library is being retired

The debut of CyberGeek has allowed ISPG to re-evaluate the way we publish and manage our core documents. The ISPG Policy Team reviewed the whole list of documents in the Information Security and Privacy Library and determined that many of them did not reflect the current-state of both system management and information delivery at CMS. As a result, the Policy Team made decisions about how to proceed with each document – and we're now referring to the remaining space as the Legacy Library. You may have noticed that the Legacy Library is looking a little sparse these days. That's on purpose! Many of your frequently-used documents and templates have transitioned to CyberGeek. If there's something specific you're looking for, try using the Search feature on the ISPG website.

Some templates are now on CyberGeek

Good news, everyone! You can find many of the templates you use every day on CyberGeek. Having the templates directly on the site will allow us to:

- Reduce issues with template versioning
- Provide confidence that the information on the template is accurate and current
- Support ISPG's current processes and standards

Using templates on CyberGeek is easy. You can **use the search function** or table of contents on a page to find the template you need, then simply **copy and paste** the content into a document on your computer. You can read about all the templates that have moved from the Legacy Library to CyberGeek, while other templates are now managed in other systems (such as CFACTS).

We hope you love the new CyberGeek. As the site continues to grow, we constantly iterate to improve the information, tools, and resources better. You can expect frequent updates to the site over the next few months – check back often to see what's new.

If you have questions or would like to contact the CyberGeek team, you can find us on Slack at **#ispg-cybergeek**.

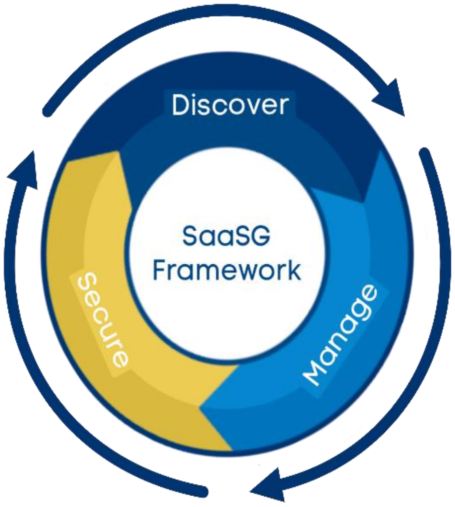
Meg Murray (Contractor, Fearless) is a Content Designer on the CyberGeek Project. She is part of the team that created the new home for ISPG at security.cms.gov. You can find Meg and the rest of the CyberGeek Team on CMS Slack at #ispg-cybergeek.

SaaSG Adoption of the Rapid Cloud Review (RCR) Policy in CMS IS2P2

Erica Rebstock and Malachi (Mal) Robinson

Software-as-a-Service (SaaS) is a cloud deployment model in which applications hosted by a third-party cloud provider, such as Amazon Web Services (AWS), are made available to consumers. The consumer typically has limited control over application configurations, and the applications are delivered to end users via the web.

Executive Order (EO) 14028, Improving the Nation's Cybersecurity (May 12, 2021), directs the Federal Government to accelerate the movement to secure cloud services and the software supply chain, including SaaS. While Federal cloud authorization frameworks, such as FedRAMP, have existed for some time, the process has not kept pace with the Federal Government's rate of cloud adoption or has considered circumstances in which FedRAMP is not always the best path for the SaaS use case.



At the outset of the SaaSG program, ISPG identified three (3) critical gaps impacting SaaS consumption and usage at CMS.

1) There was no comprehensive, centralized, and compliance-focused inventory of SaaS being consumed across CMS.
2) There were no clearly defined processes for Business Owners' requests to bring a new SaaS product and/or service into the CMS environment.
3) There was no centralized monitoring for the security posture of each SaaS product in use at CMS.

To close these gaps, the SaaS Governance team provides a secure and vetted framework to Discover, Manage, and Secure SaaS across the Agency. Further, through our Rapid Cloud Review (RCR) process, SaaSG serves as an initial risk assessment and, ultimately, where feasible, a determinant of FedRAMP readiness for CMS-consumed SaaS.

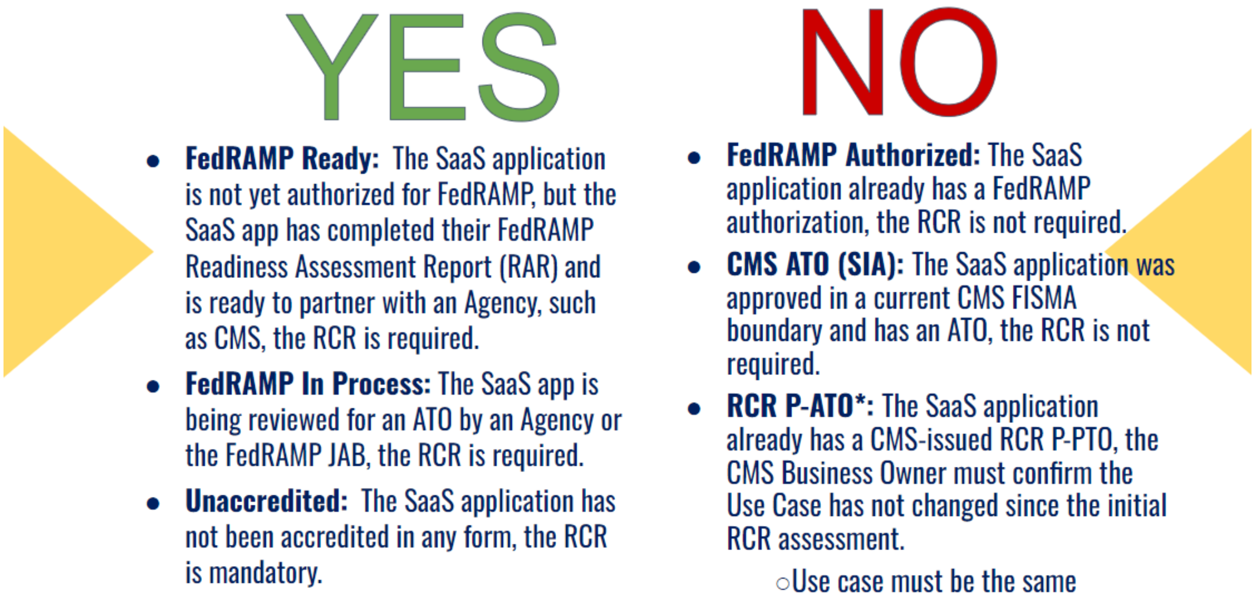
Our team has discovered significant SaaS usage across CMS in the past year. To date, SaaSG has discovered approximately 227 SaaS applications – of which 49, or 22%, are managed compared to 178, or 78%, unmanaged. In effect, this has prompted some meaningful discussions with various CMS stakeholders to strategize how we can refine our procurement practices around SaaS, foster more accountability and ownership, implement the best security practices to secure, manage, and continuously monitor SaaS, and more broadly, reduce the risk of leveraging unauthorized and non-compliant SaaS in the CMS environment.

The SaaSG program has dramatically benefited CMS by establishing a codified process for accepting new SaaS requests and evaluating those requests to support the CMS Authorizing Official (AO) in making a risk-informed decision on a SaaS product before it is authorized for use at CMS.

The SaaSG team has worked closely with the ISPG Privacy and Policy team to provide CMS leverage to mandate that SaaS products undergo an RCR to assess a SaaS vendor's risk posture, security program maturity, and FedRAMP readiness. With their guidance, we were able to draft a policy change that aligns with the overarching HHS Information Systems Security and Privacy Policy (IS2P) and CMS IS2P2 by including the following clause (highlighted):

- CMS-CLD-1: All cloud service implementations used within a FISMA system must have an approved Federal Risk and Authorization Management Program (FedRAMP) Authorization and CMS-issued ATO.
- CMS-CLD-1.1: If a Software as a Service (SaaS) product does not have a current FedRAMP authorization, a Rapid Cloud Review (RCR) and a CMS-issued Provisional Authority to Operate (P-ATO) would be needed to assess FedRAMP readiness.
    - P-ATO is an ATO to "evaluate" the use of the SaaS tool.

In essence, if your SaaS is not FedRAMP approved, you will most likely need to go through the RCR process to obtain a P-ATO. So next, you might be wondering, do I need an RCR? Here is a quick list to help determine where your SaaS might fall.



YES

- **FedRAMP Ready:** The SaaS application is not yet authorized for FedRAMP, but the SaaS app has completed their FedRAMP Readiness Assessment Report (RAR) and is ready to partner with an Agency, such as CMS, the RCR is required.
- **FedRAMP In Process:** The SaaS app is being reviewed for an ATO by an Agency or the FedRAMP JAB, the RCR is required.
- **Unaccredited:** The SaaS application has not been accredited in any form, the RCR is mandatory.

NO

- **FedRAMP Authorized:** The SaaS application already has a FedRAMP authorization, the RCR is not required.
- **CMS ATO (SIA):** The SaaS application was approved in a current CMS FISMA boundary and has an ATO, the RCR is not required.
- **RCR P-ATO*:** The SaaS application already has a CMS-issued RCR P-PTO, the CMS Business Owner must confirm the Use Case has not changed since the initial RCR assessment.
    - Use case must be the same

For future reference, this information is also available on the SaaSG CyberGeek Page here: https://security.cms.gov/learn/saas-governance-saasg.

Additionally, the SaaSG team has also developed a list of possible questions that may come up as you are determining where your SaaS lands:

I have been using my SaaS for a while now. Do I still need to do an RCR?

Yes, you will still need to complete an RCR. We are going through our list of discovered, unaccredited SaaS and will contact Business Owners using SaaS that has not yet been reviewed. Our definition of unaccredited SaaS is "*all SaaS that does not have approval through the CMS ATO approval process*." We have updated our report to include risk determinations and have incorporated routing through Service Now (SNOW) to obtain approvals from the CMS CISO and CIO. If you review our SaaS dashboard in Tableau, it may say *unaccredited* for some RCRs that we reviewed a while ago, and that is because even though those were reviewed, they were never officially pushed through the SNOW process.

What if I complete an RCR and my SaaS is deemed High Risk?

If your SaaS risk determination is deemed High, you will most likely not obtain the CMS AO's approval. You will need to work with your Cyber Risk Advisor (CRA) and Information Systems Security Officer (ISSO) to understand the issue making the risk High. You may also have to work with the SaaS vendor to see if any mitigations can be implemented to reduce the risk and bring it into an acceptable risk threshold.

Can I use a SaaS that has already been through the RCR Process?

Absolutely! If the use case is the same as the initial RCR assessment, you will not need to repeat the RCR process. However, if the RCR was completed more than six (6) months ago, we will contact the SaaS vendor for updated security artifacts (e.g., SOC2, penetration test report, etc.) to see if there are any deltas in the results.

What if my SaaS was included in my FISMA ATO boundary and was already approved?

Then, you do not need to go through the RCR process. However, we would still like to know and track that on our inventory list in case another CMS Business Owner/Application User is looking to use the same SaaS application.

It has been determined that my SaaS will never be suitable for FedRAMP authorization; how often will my SaaS have to undergo an RCR evaluation for continued authorization/use at CMS once the policy is in place?

SaaS that is unsuitable for a FedRAMP authorization and deemed low or moderate risk will go through the ATO approval process and obtain a P-ATO from the CMS AO. It will then be placed into the continuous monitoring process and, as a result, will have continuous authorization. Minimally, we will reassess the SaaS annually unless the use case changes that would warrant a more frequent evaluation.

We understand that many CMS business application owners and users will have more questions about how this will impact their program and/or services. To help alleviate this concern, we have implemented a Communication Plan to socialize the policy change throughout CMS. We hope that through our socialization, we can obtain customer feedback and, more importantly, ensure transparency when these types of changes occur. In the past couple of months, we have presented at several CMS forums (e.g., CMS Cybersecurity Community Forum (C3F), Shared Services Board (SSB), SaaS Office Hours, etc.) and plan to continue to do so in the New Year. Additionally, we will utilize the SWIFT process for our official comment request following a meeting with other groups across CMS. We anticipate the formal adoption of the RCR policy into the IS2P2 by February 2024.

If you have determined that you would like to proceed with procuring a SaaS application or have further questions regarding guidance on how to evaluate a SaaS application, please contact the SaaS Governance team at saasg@cms.hhs.gov or join our CMS Slack Channel at #ISPG-SaaS-governance.

Erica Rebstock is with Aquia, Inc. and currently serves as the Program Manager for the SaaSG team in ISPG. Erica is CISSP certified with a Master of Science (M.S.) in Cybersecurity and Information Assurance from Western Governors University. She comes to CMS with a 17+ year background in Information Assurance and Cybersecurity. Her experience ranges from a Civil Servant with the U.S. Army and U.S. Navy to a Department of Defense consultant specializing in Governance, Risk, and Compliance (GRC), Risk Management Framework Accreditations, Validation, and Penetration testing.

Malachi (Mal) Robinson is with CMS and currently serves as the Federal Lead for the SaaSG and FedRAMP PMO programs in ISPG. Malachi is CISSP and FAC P-PM II certified with a Master of Science (M.S.) in Cybersecurity from Marymount University. Malachi has been with CMS for nearly a decade and is widely known for his program management, CPIC, and security expertise with the CMS Identity Management program in OIT.

Phishing-Resistant MFA: A Critical Need in 2024

Sean Patnode

As 2024 approaches, the cybersecurity landscape rapidly evolves, underscored by the 2023 Verizon Data Breach Investigations Report (DBIR) findings. This report reveals a worrying surge in social engineering attacks, with Business Email Compromise (BEC) accounting for more than half of reported incidents. This trend reflects the growing sophistication of cyber threats and highlights the vulnerabilities introduced by the shift towards remote and hybrid work environments. More alarmingly, human error remains a significant factor, playing a role in 74% of breaches. These insights paint a clear picture: attackers are increasingly adept at exploiting human vulnerabilities, and there's an urgent need for more proactive defense strategies.

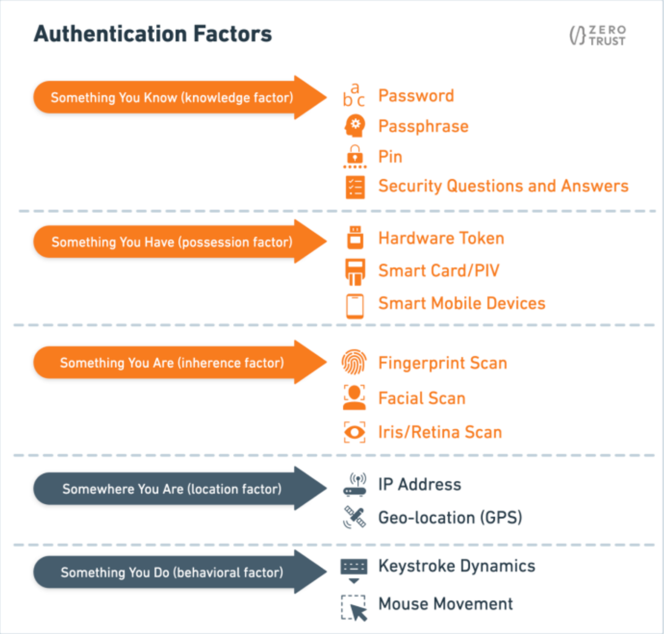
In this context, organizations must pivot towards two critical areas of improvement. Firstly, there's a pressing need to enhance workforce awareness and training related to evolving threats. Secondly, and perhaps more crucially, there is a need to implement advanced security measures like Phishing-Resistant Multi-Factor Authentication (PR-MFA). These technologies are not just about adding layers of security–they represent a paradigm shift in how we approach cybersecurity. By securing user identities, PR-MFA significantly reduces the reliance on users to detect threats, thereby fortifying the organization's overall security posture.

Multi-Factor Authentication: A Primer for Phishing-Resistant Concepts

Multi-factor authentication (MFA) is pivotal in ensuring identity security, requiring users to present two or more authentication factors before granting access. The factors typically encompass:

- Something You Know
- Something You Have
- Something You Are

The foundational concept of MFA is its emphasis on layered security through redundancy–meaning that if one authentication factor, such as a password, is compromised, additional factors ensure continued protection.

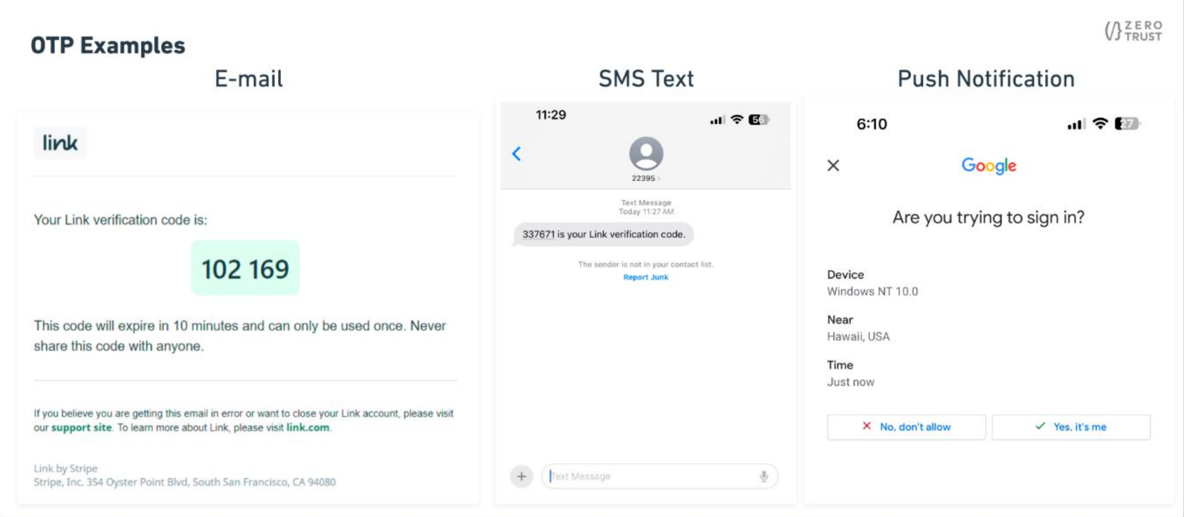

Authentication Factors
ZERO TRUST
Something You Know (knowledge factor)
Password
Passphrase
Pin
Security Questions and Answers
Something You Have (possession factor)
Hardware Token
Smart Card/PIV
Smart Mobile Devices
Something You Are (inherence factor)
Fingerprint Scan
Facial Scan
Iris/Retina Scan
Somewhere You Are (location factor)
IP Address
Geo-location (GPS)
Something You Do (behavioral factor)
Keystroke Dynamics
Mouse Movement

The evolution of MFA has consistently sought to strike a balance between robust security and user convenience. Overly complex systems can lead to poor user compliance, weakening the overall security posture. Therefore, the most effective MFA systems provide robust security measures while maintaining ease of use for the end user.

Popular MFA Methods in the Era of Smart Devices

As MFA has evolved, two methods have gained widespread popularity, primarily due to their ease of implementation and the increasing prevalence of smart mobile devices.

One-Time Password (OTP): These unique, single-use codes are valid for one session or transaction and can be delivered via email, SMS, or smartphone notifications. They provide temporary access privileges that expire after use.


OTP Examples

E-mail

link

Your Link verification code is:

102 169

This code will expire in 10 minutes and can only be used once. Never share this code with anyone.

If you believe you are getting this email in error or want to close your Link account, please visit our support site. To learn more about Link, please visit link.com.

Link by Stripe
Stripe, Inc. 354 Oyster Point Blvd, South San Francisco, CA 94080

SMS Text

Text Message
Today 11:27 AM

337671 is your Link verification code.

The sender is not in your contact list.
Report Junk

Push Notification

Google

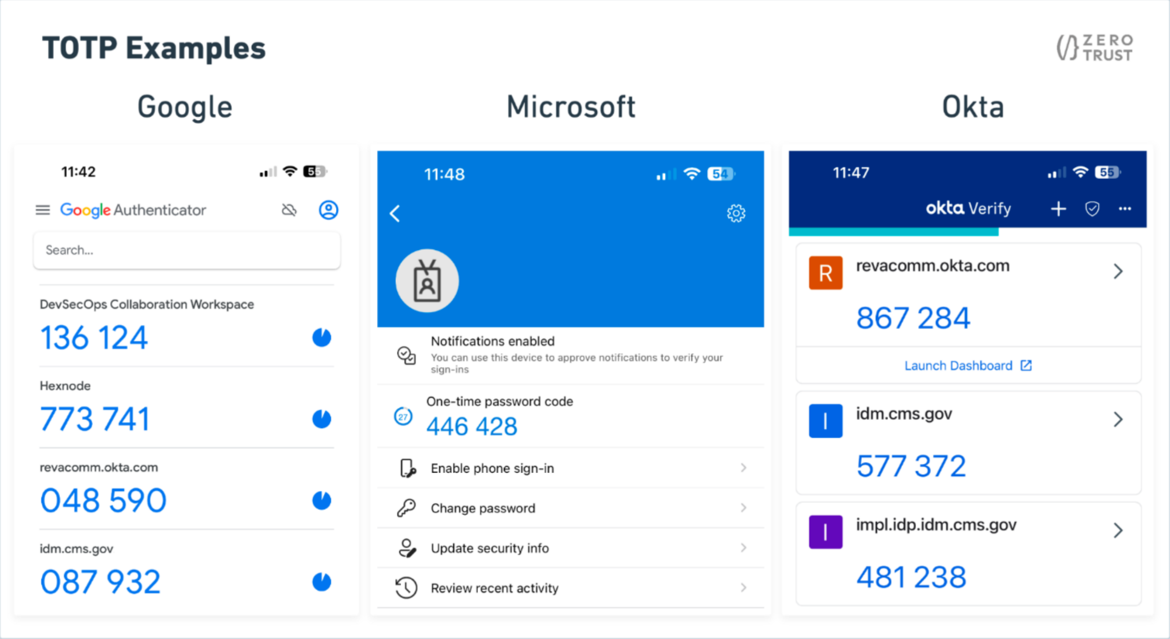
Are you trying to sign in?

Device
Windows NT 10.0

Near
Hawaii, USA

Time
Just now

Time-based One-Time Passwords (TOTP): Similar to OTPs, TOTPs are algorithmically generated and valid for a short period, typically 30 seconds to a minute. Used in mobile authenticator apps like Google, Microsoft, and Okta, TOTPs offer a dynamic password for enhanced security.


TOTP Examples

Google

DevSecOps Collaboration Workspace
136 124

Hexnode
773 741

revacomm.okta.com
048 590

idm.cms.gov
087 932

Microsoft

Notifications enabled
You can use this device to approve notifications to verify your sign-ins

One-time password code
446 428

Okta

revacomm.okta.com
867 284

idm.cms.gov
577 372

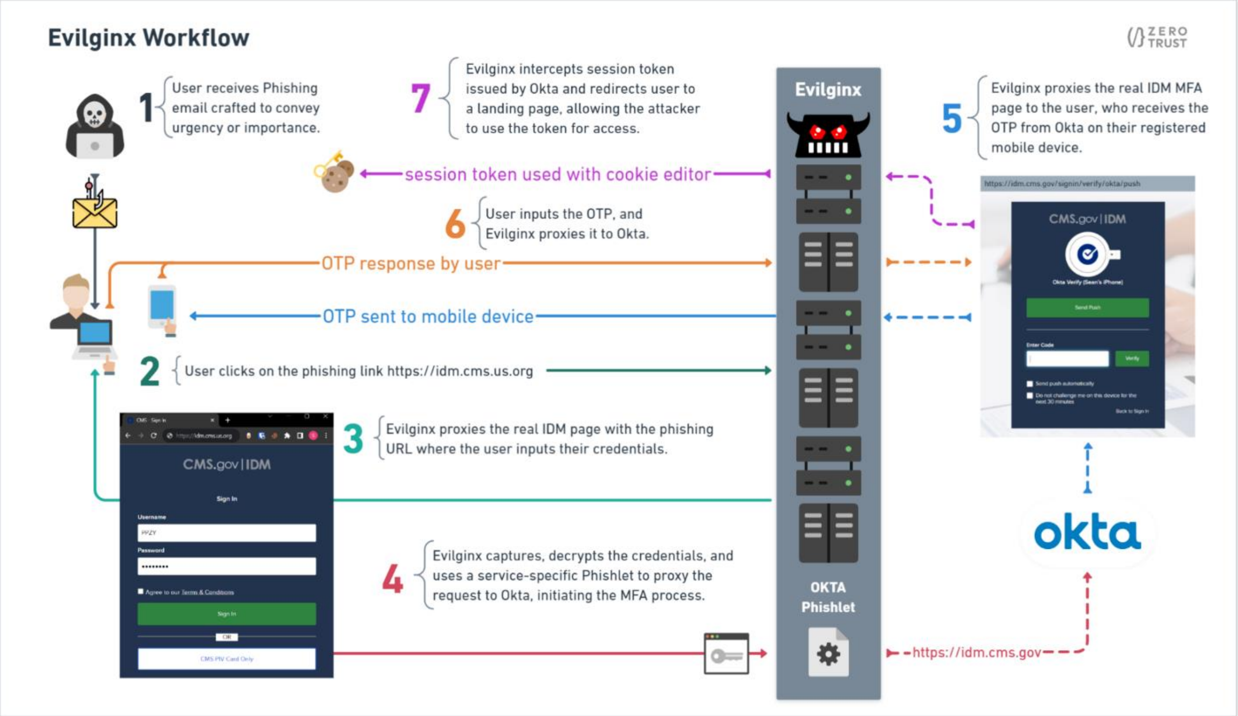
impl.idp.idm.cms.gov
481 238

OTP and TOTP MFA approaches have significantly improved authentication security. Still, Despite MFA's advancements and widespread adoption, sophisticated open-source tools like Evilginx (see below) have simultaneously escalated the threat of phishing and social engineering attacks.

Understanding User Vulnerability: The Case of Evilginx

Evilginx is a man-in-the-middle (MITM) attack framework that elevates phishing techniques beyond the conventional template-based fake sign-in pages. It functions as a reverse proxy by strategically presenting, decrypting, and intercepting sensitive data between the user and a legitimate website. This sensitive data includes usernames, passwords, and, more importantly, authenticated session tokens. With this capability, Evilginx effectively circumvents established MFA methods and poses a formidable challenge to security-fatigued users.

The diagram below illustrates the operation of Evilginx in circumventing Okta OTP, using CMS IDM as the example scenario.


Evilginx Workflow
ZERO TRUST
1 User receives Phishing email crafted to convey urgency or importance.
7 Evilginx intercepts session token issued by Okta and redirects user to a landing page, allowing the attacker to use the token for access.
Evilginx
5 Evilginx proxies the real IDM MFA page to the user, who receives the OTP from Okta on their registered mobile device.
session token used with cookie editor
https://idm.cms.gov/signin/verify/okta/push
CMS.gov | IDM
Okta Verify (Sean's iPhone)
Send Push
Enter Code
Verify
Send push automatically
Do not challenge me on this device for the next 30 minutes
Back to Sign In
6 User inputs the OTP, and Evilginx proxies it to Okta.
OTP response by user
OTP sent to mobile device
2 User clicks on the phishing link https://idm.cms.us.org
CMS - Sign In
https://idm.cms.us.org
CMS.gov | IDM
Sign In
Username
PPZY
Password
Agree to our Terms & Conditions
Sign In
OR
CMS PIV Card Only
3 Evilginx proxies the real IDM page with the phishing URL where the user inputs their credentials.
okta
4 Evilginx captures, decrypts the credentials, and uses a service-specific Phishlet to proxy the request to Okta, initiating the MFA process.
OKTA Phishlet
https://idm.cms.gov

Let's delve into how Evilginx operates at a crucial stage – step 3 – where the unsuspecting victim inputs their credentials into the legitimate CMS IDM login page which is reverse proxied from Evilginx (https://idm.cms.us.org). Unlike traditional phishing attacks, which MFA typically thwarts, Evilginx presents a more sophisticated threat. Here's a step-by-step breakdown of this deceptive process:

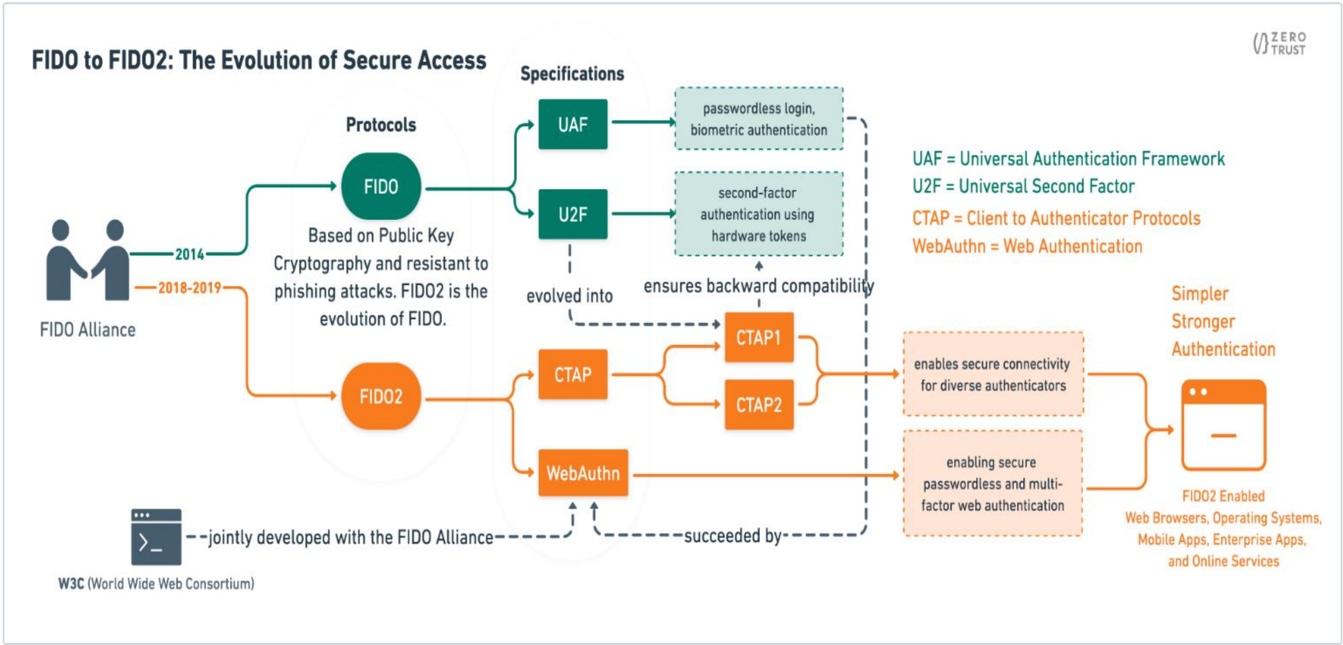
1. **Credential Verification**: The phishing URL, skillfully disguised as the real CMS IDM login URL, starts by verifying the entered credentials against the actual CMS IDM system.
2. **MFA Challenge Response:** The user, believing they are securely interacting with the legitimate site, completes the MFA challenge.
3. **Session Token Creation**: Okta generates a session token in response to the completed MFA challenge. This token is usually in the form of a browser cookie or JSON Web Token.
4. **Evilginx's Strategic Maneuver**: At this critical moment, Evilginx intercepts the session token and subtly redirects the user to a different page, commonly known as a 'phishing URL'.
5. **Gaining Unauthorized Access**: The attacker exploits this situation by injecting the stolen session token into their web browser, bypassing the MFA, and gaining unauthorized access to the victim's account.

6. Duration of Unauthorized Access: The extent of this unauthorized access depends on when the session token is revoked. Revocation could happen if the user logs out of IDM or when the token expires per the Okta session policy. Typically, these policies are set for extended durations for user convenience, potentially extending the attacker's access.
7. Potential for Further Compromise: With the victim's username and password already in their control, the attacker can further exploit the situation. They can add additional MFA methods during this initial breach without phishing the user again.

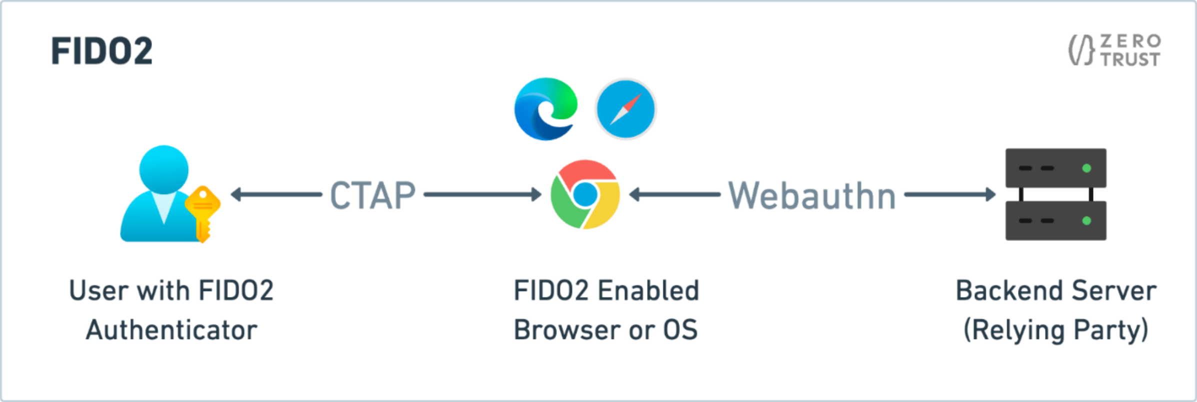
Identifying sophisticated attacks like Evilginx and the phishing URLs they create can be daunting, particularly for individuals new to an organization, such as recent hires or contractors. Historically, the responsibility has fallen on each person to discern between legitimate and fraudulent domains – a task fraught with risk for many organizations. Thankfully, advancements in technology offer robust solutions to this challenge. Among these, FIDO2 stands out as a pioneering force in enhancing online identity security, offering practical tools to counteract the threat of deceptive websites.

The FIDO Alliance: Pioneering Enhanced Authentication Standards

The FIDO (Fast Identity Online) Alliance, founded in 2012, epitomizes a concerted effort to transcend traditional password-based security, aiming to establish more robust authentication standards. By pioneering innovative protocols such as UAF (Universal Authentication Framework) and U2F (Universal 2nd Factor), the Alliance has been instrumental in laying the foundational framework for public key cryptography. FIDO2, the most sophisticated iteration of FIDO methodology, enables users to authenticate their identity securely without relying on passwords, utilizing advanced methods like biometrics or physical security keys.


FIDO to FIDO2: The Evolution of Secure Access
ZERO TRUST
Protocols
Specifications
FIDO Alliance
2014
2018-2019
FIDO
Based on Public Key Cryptography and resistant to phishing attacks. FIDO2 is the evolution of FIDO.
FIDO2
UAF
U2F
passwordless login, biometric authentication
second-factor authentication using hardware tokens
evolved into
ensures backward compatibility
CTAP
CTAP1
CTAP2
WebAuthn
enables secure connectivity for diverse authenticators
enabling secure passwordless and multi-factor web authentication
UAF = Universal Authentication Framework
U2F = Universal Second Factor
CTAP = Client to Authenticator Protocols
WebAuthn = Web Authentication
Simpler Stronger Authentication
FIDO2 Enabled Web Browsers, Operating Systems, Mobile Apps, Enterprise Apps, and Online Services
jointly developed with the FIDO Alliance
succeeded by
W3C (World Wide Web Consortium)

FIDO2's innovative approach to combating phishing lies in its ability to verify cryptographic keys and user presence verification during the MFA process, making stolen credentials useless and phishing attacks ineffective. In light of tools like Evilginx, FIDO2's PR-MFA emerges as an effective countermeasure.


FIDO2
ZERO TRUST
CTAP
Webauthn
User with FIDO2 Authenticator
FIDO2 Enabled Browser or OS
Backend Server (Relying Party)

Securing the Future: Implementing FIDO2 and Phishing-Resistant MFA in 2024

Adopting Phishing-Resistant Multi-Factor Authentication (PR-MFA) technologies like FIDO2 is challenging. A comprehensive discovery and research phase is essential, starting with security and feasibility assessments, testing and deployment among high-risk or privileged access users like administrators, and gradually extending to the broader workforce. This approach is being piloted within the batCAVE through the FIDO2 YubiKey Pilot initiative, led by Elizabeth Schweinsberg in collaboration with the CMS FIDO2 Task Force.

In conclusion, FIDO2 enhances security by authenticating domain legitimacy through public key cryptography, removing the need for password-based security, and reducing human error risk. With strategic planning, phased testing, and implementation of PR-MFA, organizations like CMS can significantly bolster their security posture and enhance user experience in identity security. This innovation establishes a new gold standard for Authentication Security, providing a formidable shield against sophisticated phishing tools like Evilginx2 and heralding a new era in cybersecurity resilience.

Sean Patnode works for RevaComm and is a Lead Security Engineer for the Zero Trust Team in the batCAVE platform.

Be on the Lookout for Those Phishing Traps!

Saad Zulqadar

Over the past couple of weeks there has been an increase in the number of phishing emails received by CMS employees. The emails are designed to make users click on a link or an attachment. They may contain themes such as a "shared document" that needs review or an outstanding invoice that needs to be paid.

Once the user clicks the link or attachment, they are sent to a login page. The login page usually resembles a Microsoft login page, but this can vary based on the phishing theme being used. These types of phishing emails are known as credential harvesting emails and once a username and password are submitted to the login page, the attacker can attempt to use them to gain access to protected information and resources.

Please remain vigilant when you are opening emails. Taking a minute to check for valid senders or to check the destination of any embedded links (by hovering over them with your cursor) can help protect your credentials against these types of phishing emails.

If you do receive a suspicious email, do not click any links or open any attachments. Report the email by clicking the "Report Phishing" or "Report Spam" button on your Outlook toolbar or by sending it to spam@cms.hhs.gov.

Welcome to a New Way of Learning all Things Cybersecurity

Saad Zulqadar

Has CMS hired a group of actors? Not quite! In the era of technological marvels and mind-boggling innovations, CMS is embracing the future with open arms. Enter Synthesia – the AI software that's set to revolutionize CMS training, turning mundane learning sessions into a spectacle that's as entertaining as a magic show but way more practical.

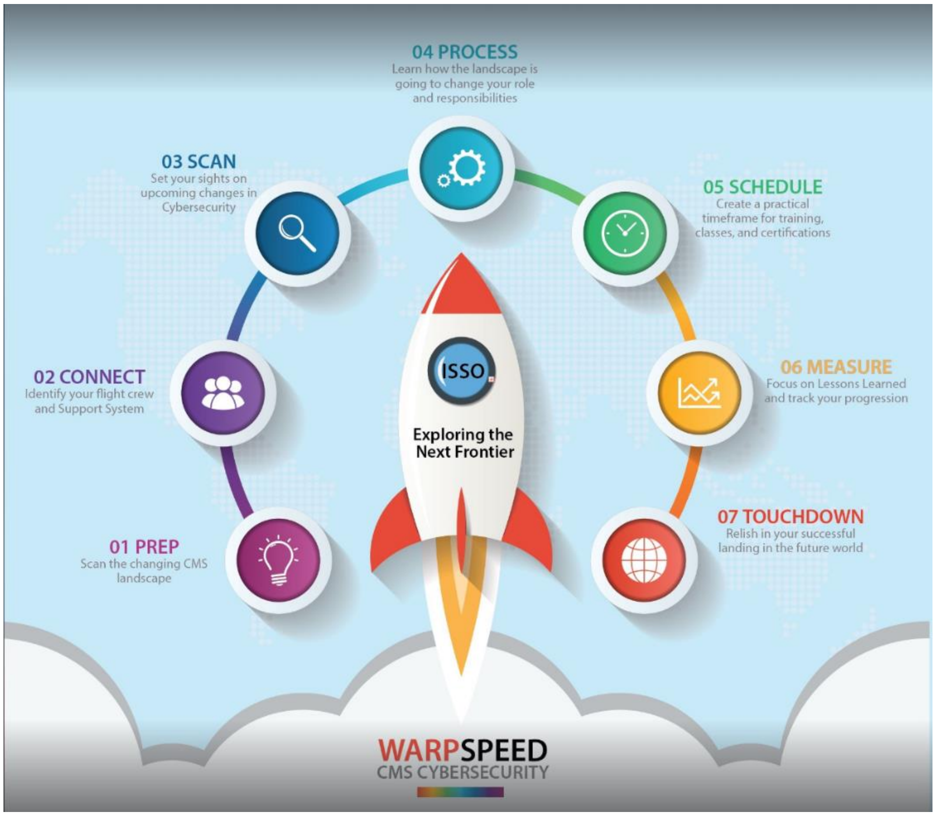
Gone are the days of the snooze-inducing PowerPoint presentations and yawn-worthy instructional videos that made even the most dedicated employees question their life choices. With Synthesia, CMS training takes a futuristic leap into the realm of Artificial Intelligence.

Embrace a future where your training sessions are as captivating as binge-watching your favorite series. CMS training just got a futuristic makeover! Get ready to learn and revolutionize your learning experience with Synthesia's AI magic!

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

ISSO – Exploring the Next Frontier

Allison Schiller and Christopher David



04 PROCESS
Learn how the landscape is going to change your role and responsibilities

03 SCAN
Set your sights on upcoming changes in Cybersecurity

05 SCHEDULE
Create a practical timeframe for training, classes, and certifications

02 CONNECT
Identify your flight crew and Support System

ISSO
Exploring the Next Frontier

06 MEASURE
Focus on Lessons Learned and track your progression

01 PREP
Scan the changing CMS landscape

07 TOUCHDOWN
Relish in your successful landing in the future world

WARPSPEED
CMS CYBERSECURITY

As we prepare to blast into the next frontier of information security, let's take a moment to complete our pre-flight **PREP** and view the landscape around us, the CMS environment as it exists now. There are two phases of the prep that we'd recommend. First, **SCAN** the CMS environment and assess what is around the corner in terms of new processes, data, and initiatives. For example:

- Security Data Lake awareness and orientation
- Core CRM Dashboards
- Zero Trust, Enhanced Vulnerability Scoring
- SIGNAL, Batcave, SaaSg, CAPM

Second, focus on the **PROCESS** of how the landscape is going to change your role and responsibilities as an ISSO. Most ISSOs work daily in the CFACTS environment to view and log the data you need to complete your work, and many of you are already comfortable with the Tableau dashboards. Some of the challenges in the current environment include finding and utilizing demos and trainings, learning about the various tools in your toolkit, and keeping up with changing processes, including the ATO Processes and Federal Reporting.

Remember that a key part of ensuring success in your journey are the members of your team, and we encourage you to **CONNECT** with CMS staff via Slack, email, and other regular meetings such as the C3 Forum, the CyberRisk Corner, and the ISPG Demo Days. All of these are great venues to identify your flight crew and to tailor your support system in response to changes.

As you can see, this isn't your parent's space suit – we are entering exciting new territory and are equipped with all the latest gear. This is where we begin to enter warp speed, and we want to be sure each pilot is aware of what is to come. Your new toolkit includes:

- CMS Learning Management System (LMS) Centralization – tracking what's available for learning and what each pilot has done so far.
- Just in Time learning – short, focused videos to get you up to speed quickly. These videos are designed to give you practical "How To" instructions and should be seen as a supplement to more in-depth study.
- ISSO Certifications.
- Enhanced Communications & Outreach - CyberGeek, C3 Forum, Cyber Risk Corner.

Melinda Burgess and the CyberGeek team have developed some great resources for ISSOs:

ISSO Handbook
This is the go-to resource for ISSOs both new and experienced. Here you can find resources for ISSO onboarding, training, support, community, and an overview of the role and its responsibilities.

CMS Security and Privacy Handbooks
You may already know that the Risk Management Handbook (RMH) is being phased out. It will be replaced with the new updated series: CMS Security and Privacy Handbooks. These handbooks provide procedural guidance to help you meet control requirements and perform necessary cybersecurity tasks.

Search for ISSO resources
Use the Search page to find and filter all the information available on CyberGeek. The filters allow you to narrow down to specific resource types, topics, or role-based information.

New online templates
ISSOs use a lot of templates in their daily work - so you'll want to review this post from the Policy Team to see how template management is changing at ISPG. Instead of versioned PDFs, you can now access templates on the ISPG website and copy them with confidence into your own Word doc, knowing it is the most recent version.

ISPG News and Updates (blog)
The ISPG blog is now the place to go for timely updates from the policies, programs, and tools you use every day as an ISSO. Use the "Publisher" filter at the top of the blog to see posts from specific teams at ISPG (such as Policy, CFACTS, SaaS Governance, ACT, and more.)

As we head into the new and changing frontiers, it is increasingly important to have a **ROADMAP** and **SCHEDULE**, a clear path to guide each pilot's training needs. The journey can be overwhelming, so we encourage leveraging the new LMS as a One Stop site in creating a tailored set of courses, training classes, and assessments. The LMS is also where you will be able to **MEASURE** your progression through the courses and proactively monitor learning opportunities as they become available. In addition, a candid assessment of your flight training should include a focus on Lessons Learned and any **COURSE CORRECTIONS**, if needed.

As this flight comes to an end, and we **TOUCHDOWN** at our desks, we can look back at what we saw along the way: our journey introduced a clear map of new systems and tools: updated learning management, dashboards, and the security data lake. We have seen what is out there, and we know what we need to be able to engage and succeed in the new frontier.

Allison Schiller is the Human-Centered Design Specialist for the Reporting & Data Integration Team at the Division of Implementation and Reporting.

Christopher David is the Program/Project Manager (Enterprise Cybersecurity Program Support and ISSOaaS Program). He is an active member of the Reporting & Data Integration team at the Division of Implementation and Reporting.

Supply Chain Risk Management (SCRM) at CMS and Across the United States Federal Government.

Billy Hayes and Michael Hobert

According to AP News, on November 27th President Biden convened the nation's first supply chain resilience council. Part of this agenda included leveraging the Defense Production Act to increase the Department of Health and Human Services' budget to onshore manufacturing for certain medications deemed crucial for U.S. National Security. Additionally, the agenda included a cross-departmental initiative to share supply chain information. This council convened a week before the Federal Acquisition Regulation (FAR) Interim Rule – Implementation of Federal Acquisition Supply Chain Security Act (FASCSA) goes into effect.

This article has three objectives. The first objective is to contextualize this Presidential-level attention on Supply Chain Risk Management (SCRM is pronounced "*skrim*" by its practitioners) which will include a brief cyber perspective. The second objective is to outline SCRM components and considerations that are essential across all Federal agencies. The third objective is to showcase how CMS is on the leading edge of many of these foundational principles and share how CMS SCRM assessments can be requested.

In today’s highly connected, interdependent world, all organizations rely on others for critical products and services. This reliance is further compounded by a delicate global relay race where efficiency is crowned king. In a “just-in-time” logistics framework, suppliers provide goods or services at exactly the moment of need. However, the reality of globalization, while providing many benefits, has resulted in a world where organizations no longer fully control – and often do not have visibility into – the full extent of the complex and dynamic networks that support their supply chain ecosystems. The COVID-19 pandemic exposed the catastrophic effects brought on when previously unknown links along a given supply chain were overwhelmed and broken. Today, as known links become threatened by increased geopolitical and natural-disaster events, supply chains are becoming increasingly threatened by the ubiquity of cyber threats.

With more businesses procuring digital products and services, and moving their workloads to the cloud, the impact of a cybersecurity event is greater than ever and could include personal data loss, significant financial losses, compromise of product integrity or safety, and even loss of life! Organizations can no longer protect themselves by simply securing their own infrastructures -- because their electronic perimeter is no longer meaningful; threat actors intentionally exploit the weaker link(s) in a supply chain by targeting the suppliers of more cyber-mature organizations.

Key components and considerations for a comprehensive approach to Supply Chain Risk Management across the U.S. Federal Government include:

1. **Policy and Governance**
    - Define and establish a comprehensive SCRM policy framework.
    - Designate responsibility and accountability for SCRM at various levels of the organization.
    - Align SCRM efforts with broader government policies and directives.

2. **Risk Assessment**
    - Conduct thorough risk assessments to identify and analyze the totality of potential risks for a given supplier before they enter the supply chain.
    - Assess both physical and cybersecurity risks associated with suppliers.
    - Evaluate the criticality of supply chain components and their impact on mission objectives.

3. **Supplier Management**
    - Establish a centralized repository of suppliers and assess their reliability and security posture.
    - Develop and maintain relationships with key suppliers to enhance transparency and communication.

4. **Cybersecurity Measures**
    - Implement cybersecurity measures to protect against cyber threats, such as data breaches, malware, and ransomware attacks.
    - Encourage the adoption of cybersecurity best practices by suppliers.
    - Regularly assess and audit the cybersecurity practices of suppliers.

5. **Information Sharing, Compliance, and Collaboration**
    - Ensure compliance with relevant laws, regulations, and standards related to supply chain security.
    - Stay updated on changes in regulations and adjust SCRM practices accordingly.
    - Collaborate with regulatory agencies to address compliance challenges.

6. **Continuous Monitoring**
    - Implement continuous monitoring mechanisms to detect and respond to emerging risks within the supply chain.
    - Utilize advanced analytics and technology to monitor and assess the health of the supply chain in real-time.
    - Establish incident response plans to address disruptions promptly.

7. **Resilience Planning**
    - Develop and maintain contingency plans to address supply chain disruptions.
    - Test and update resilience plans regularly to ensure effectiveness.
    - Establish redundancy and alternative sourcing strategies to mitigate risks.

8. **Training and Awareness**
    - Provide training to personnel involved in supply chain management on SCRM best practices.
    - Foster a culture of awareness and vigilance regarding supply chain risks.
    - Encourage reporting of suspicious activities or potential risks.

9. **International Collaboration**
    - Collaborate with international partners to address global supply chain risks.
    - Engage in information exchange and joint efforts to enhance supply chain security.
    - Align SCRM efforts with both industry and U.S. Government standards and best practices.

By adopting this comprehensive approach to Supply Chain Risk Management, the U.S. Federal Government can better safeguard its supply chains, enhance resilience, and mitigate the impact of potential disruptions.

The Centers for Medicare and Medicaid Services (CMS) Information Security and Privacy Group's Division of Strategic Information Supply Chain Risk Management Team (ISPG DSI SCRM) has been actively using many of the principles above to support the CMS stakeholders. The CMS SCRM team's critical capability is to ensure business resilience and prevent the introduction of weak links by identifying, assessing, and mitigating supply chain risks. CMS takes a forward leaning, multidisciplinary approach to managing these types of risks by adding a cyber lens. This approach is called *cyber* supply chain risk management (C-SCRM). (James Gimbi*, et al*., "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry," NISTIR 8276, National Institute for Standards and Technology, Feb 2021). In addition to C-SCRM, DSI also maintains a more wide-angle SCRM lens.

The Supply Chain Risk Management (SCRM) Assessment Team (A-Team) is a component within the DSI SCRM team comprised of a multidisciplinary group of SCRM professionals. The A-Team uses traditional and non-traditional SCRM tools to maintain the health of CMS' supply chain ecosystem. These tools are applied within an analytic framework designed to "*lift the fog*" of uncertainty through 360° supplier assessments. Such assessments can be deployed for companies currently within CMS' ecosystem, but they are ideally suited to be conducted **before** risks can enter CMS' supply chain. When threats are discovered, the team ensures the information is shared with all internal and external stakeholders, including across other U.S. Government agencies.

The SCRM A-Team has state-of-the-art commercial SCRM tools at the team's disposal. The team also uses a cocktail of non-traditional SCRM tools combined with open-source intelligence methodologies to identify, assess, and mitigate risks. In the dynamic world we live in, risks are an inherent cost of business, so the team recommends appropriate mitigation strategies based on CMS' acceptable risk thresholds. If new risks are discovered, the A-Team can be called upon to consult with internal stakeholders to create an acceptable mitigation strategy.

The A-Team "lifts the fog" of uncertainty through the analytic tenet framework "FOGLIPHT". We assess each supplier's…

- **Financial** health, including its solvency, as well as identifying any foreign or malign funding streams.

- **Ownership** includes the industry standard Foreign Ownership, Influence, and Control (FOCI) risk factors. This category examines everything from key leaders, partnerships with risky foreign actors, and the firm's foreign customers & partnerships.
- **Geopolitical** encompasses risk factors that could negatively impact CMS' supply chain from across this spectrum including gray zone actions, coups d'état, terrorist attacks, to full scale armed conflict.

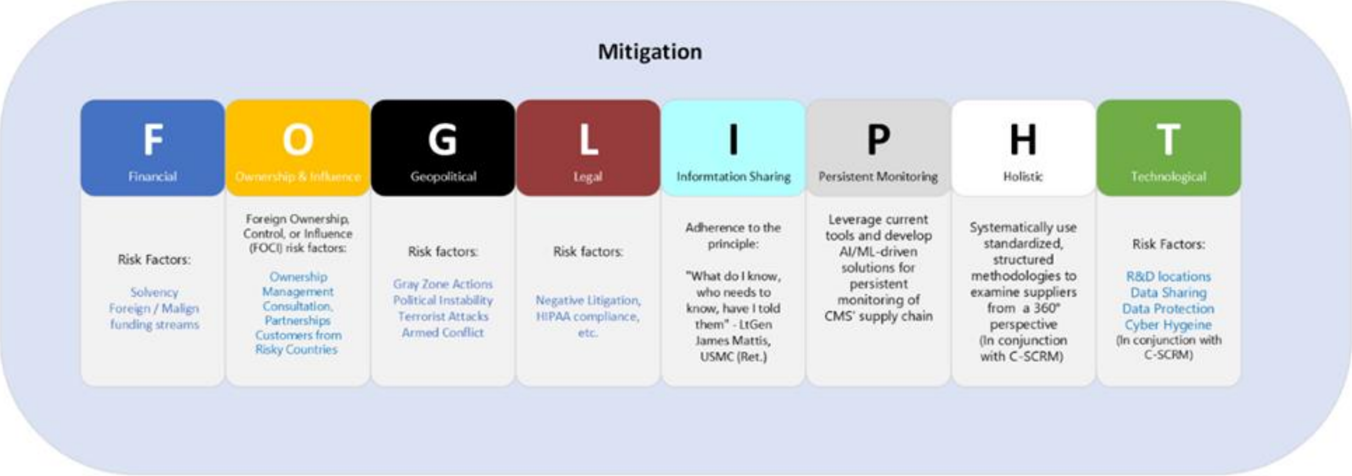
- **Legal** examines suppliers' potential or current litigation, any traces of counterfeiting, Health Insurance Portability and Accountability Act (HIPAA) compliance, among others.

- **Information sharing** is a key tenet and is designed to ensure that the A-Team notifies all stakeholders affected by a discovered risk. Powered by the team's Data Scientist,

- **Persistent Monitoring** through various tools allows the A-Team to maintain cognizance over the health of CMS' current supply chain. The goal is to push the envelope and leverage artificial intelligence, specifically machine learning to automate our processes as much as possible.

- **Holistic** approaches to SCRM assessments mean that our team is not solely focused on one niche aspect of a given supplier, rather we take a 360° perspective through our structured methodologies and partnership with the C-SCRM team.

- **Technological** factors examined by the A-Team include where a given firm conducts its Research & Development, how and where it shares and protects information, etc. This aspect is conducted alongside the C-SCRM team to the greatest extent possible.



Mitigation

F
Financial
Risk Factors:
Solvency
Foreign / Malign funding streams

O
Ownership & Influence
Foreign Ownership, Control, or Influence (FOCI) risk factors:
Ownership
Management
Consultation,
Partnerships
Customers from Risky Countries

G
Geopolitical
Risk factors:
Gray Zone Actions
Political Instability
Terrorist Attacks
Armed Conflict

L
Legal
Risk factors:
Negative Litigation,
HIPAA compliance,
etc.

I
Informtation Sharing
Adherence to the principle:
"What do I know, who needs to know, have I told them" - LtGen James Mattis, USMC (Ret.)

P
Persistent Monitoring
Leverage current tools and develop AI/ML-driven solutions for persistent monitoring of CMS' supply chain

H
Holistic
Systematically use standardized, structured methodologies to examine suppliers from a 360" perspective
(In conjunction with C-SCRM)

T
Technological
Risk Factors:
R&D locations
Data Sharing
Data Protection
Cyber Hygeine
(In conjunction with C-SCRM)

Figure 1: CMS SCRM Assessment Team Analytic Tenets

The SCRM Team is available to assist CMS stakeholders on a consultative basis as well as *ad hoc* questions and support. The SCRM Team hosts the Supply Chain Risk Management Library (where you can find a link to request a Supply Chain Vendor Risk Assessment). The ISPG DSI SCRM Team can be reached by e-mail at SupplyChainRiskManagement@cms.hhs.gov.

Billy Hayes is a Sr Consultant, Supply Chain Risk Management Analyst on the CMS ISPG DSI SCRM Team. He is a retired U.S. Marine with 23 years of service, and he is a former faculty member at National Intelligence University. E-mail:billy.hayes@cms.hhs.gov

Michael Hobert is a Consultant, Instructional Design on the CMS ISPG DSI SCRM Team. His Learning & Development experience includes several major Fortune 500 companies with additional experience in sales, marketing, and management – much of that in medical device/pharma and tech industries. E-mail: Thomas.hobert1@cms.hhs.gov

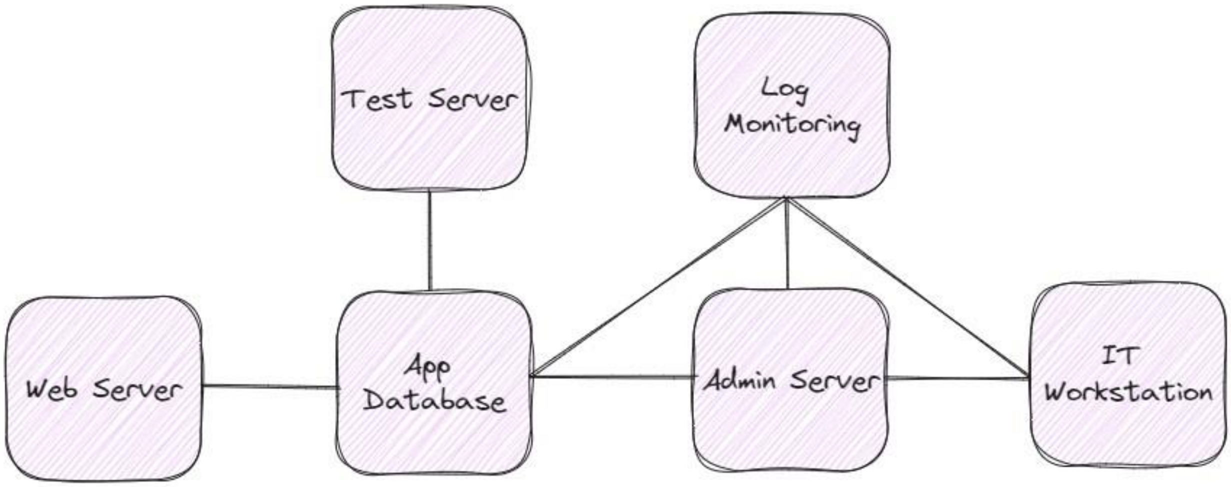
Wait, I Needed That: Criticality Analysis

Jeff Bond, Mackenzie Wartenberger, Aquia Inc.

What is important to you? More relevantly, what is important to your business? This is the question at the heart of both the Risk Management Framework and Zero Trust. Determining degrees of criticality for internal and external resources provides the basis for writing your plans, prioritizing your risk, and determining where to spend your limited money and time. A criticality analysis should be applied at the enterprise level and then incorporated into a feedback loop applying the analysis deeper and deeper; It's not always the easiest process but it is an upfront investment that pays off in the long term.

But what does this mysterious 'criticality analysis' entail? Criticality analysis is effectively all about asking questions. If you want to find the answer to the question of "What is important to the system?", you need to start by asking all the different groups of *people (stakeholders)* what matters to them. Once you have answers from all the different business groups you can start utilizing the system documentation to map the things that actually matter.

Let's apply this methodology to a simplified real-world scenario. We were already working with the IT team and requested an architecture diagram from them. It shows a self-contained environment with a development server, administrative and support servers, a database, and a web front end. Starting with this type of high-level view gives us a way to start taking small bites out of your analysis loop for determining criticality.



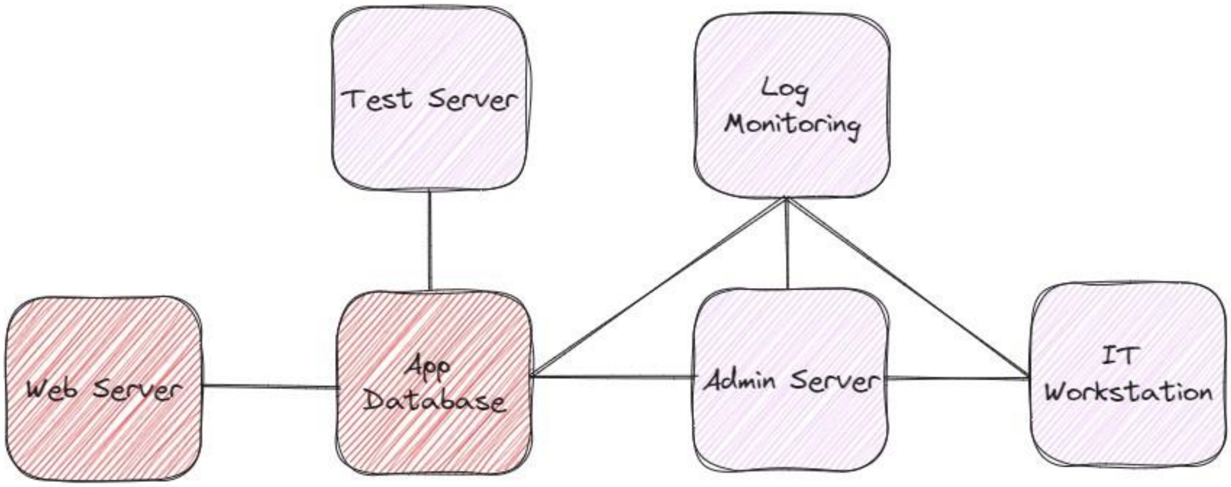
Next in this example system we will interview the following groups and obtain the following information about their relevant priorities:

- *Program Management* - Our business objective is for people to pay for and use our web app.
- *Information Technology* - Our objective is to maintain the availability of the app for users.
- *Software Engineering* - Our objective is to improve the user experience of the app.

Using this information, we can determine that from a very high level the most critical aspect of our system is the application. We have also identified two conditional truths about the application:

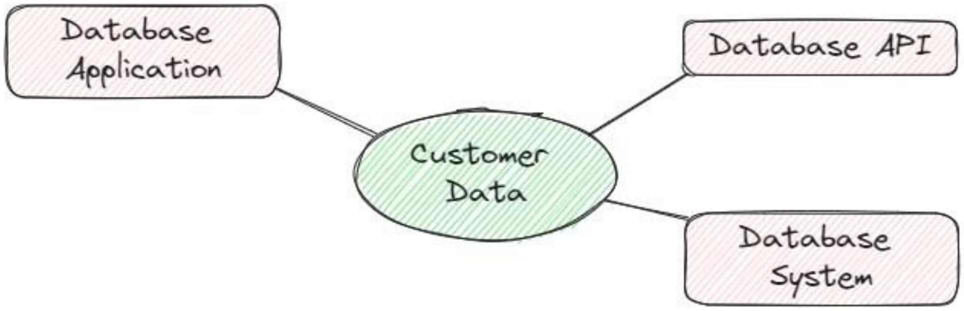
- The application depends on the app database.
- The app database does not depend on anything else.

Based off these findings, our first level analysis would produce the following diagram of critical systems (with systems shaded red as 'critical'):



By determining the truly critical systems (in our example the Web Server and Application Database, both indicated in red) we can prioritize budget and time towards protecting those resources. This obviously doesn't mean that our less critical systems can be totally ignored, as their connections could impact your critical systems, but because the critical systems in this example are not dependent on them to continue running, we can triage the efforts of our team so that we get maximum return on our investments. This type of criticality mapping is a useful but more traditional approach to managing your priorities.

Now let's consider a Zero Trust approach to Criticality Analysis. Because Zero Trust Security is premised on the ideas of least privilege and constant Authentication and Authorization, we are encouraged to look at the environment a bit differently than we previously have. In a Zero Trust criticality analysis you would break your system down into data, assets, application, and services (DAAS) and create independent "protect surfaces" for each of those systems based on their criticality. Utilizing the same example as above, one of the critical protect surfaces that we could define would look as follows.



With the information that we've already gathered from the group interviews and architecture reviews we know that customer data is one of the most critical assets that our system has. In this diagram of the protect surface for customer data we have listed the different aspects of the system that would have access to that data: Database Application, Database Application Programming Interface (API), and Database System. A main differentiator between this Zero Trust example and a traditional criticality analysis approach, is that 'system' in this example can indicate any process that accesses customer data, as opposed to the previous example where 'system' represents a physical or virtual computing environment. Using this Zero Trust criticality analysis we can identify that our critical priorities for applying security would be the systems with direct access to the customer data and allocate our resources there.

Ultimately, the goal of both of these approaches is the same: to focus security attention on the resources with the most value to the enterprise.

In order to keep this article to a shorter length than the average young adult novel, I have only gone through two very simplified examples. Using the process depicted in these examples should get you started in your journey of finding your own critical systems. As you practice and demonstrate value you can apply the process more and more granularly and with more efficiency thus increasing system security with less friction from other business groups.

Jeff Bond is a Security Architect at Aquia, Inc., supporting Elizabeth S. with Zero Trust at CMS. For almost 20 years, he has been advancing cyber security within the federal government and DoD across multiple fields including GRC, MBSE, architecture, and engineering.

A Security Architect at Aquia, Inc., supporting batCAVE Zero Trust, Mack Wartenberger is an advocate for securing the digital transformation through maturing cyber security practice in GRC, Architecture, and Zero Trust.

What's Going on With the Security Data Lake (SDL)? A Self-guided FAQ With the Latest Information Available for Cyber Risk Management Stakeholders at CMS

Jonathan Herrick, ECS

What will this article tell me about the SDL?

This article addresses the purpose of the Security Data Lake (SDL) and the capability enhancements it will provide for Cyber Risk Information Users (such as ISSOs or other members of the CMS Cybersecurity Stakeholder community), as well as the current status of the SDL launch.

Can you remind me what the SDL is and why I should care?

The Security Data Lake (SDL), spearheaded by the Information Security & Privacy Group (ISPG) in the Office of Information Technology (OIT), provides a centralized repository of cyber risk information for Users and those responsible for CMS information systems security, including those responsible for decision making regarding risk management and mitigation. The SDL includes the new Security Data Warehouse (SDW) as part of its architecture to support the Cyber Risk Management (CRM) Dashboard generation process at CMS. This new architecture and corresponding process refresh is an improvement on the previous Legacy Data Warehouse (LDW) infrastructure because it allows greater flexibility in how Users access, analyze, transform, and research the full body of available data for CMS Cyber Risk Management. Instead of having a rigid, enterprise-wide data structure, the SDL uses a flat architecture that keeps data in its native form until called upon. This data architecture allows more cost-efficient and scalable data analysis.

Ok, when can I expect to see these changes?

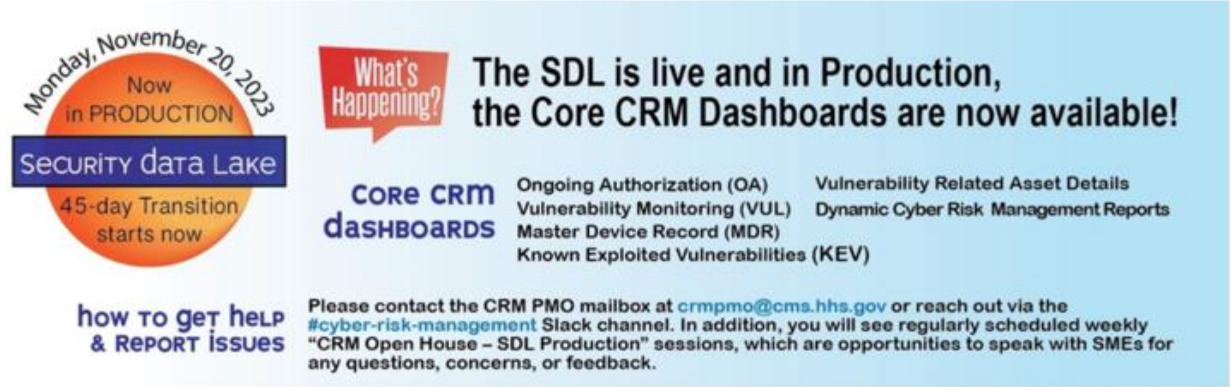
The sourcing of SDL data, and use of the updated SDW architecture for generation of CRM Dashboards, went live Monday, November 20th, and Core CRM Dashboards are now available. The new process and architecture changes are currently in a transition period, which will continue until January 2nd. As a result of the launch, you should not notice an immediate difference or change in the Cyber Risk Dashboards (such as Tableau). Instead, the new SDL will allow for CMS to build and enhance Cyber Risk Management capabilities over time, essentially setting up the agency for the future by adding back-end upgrades to how data is stored, called, accessed, and ultimately used. To that end – you can expect that there won't be any degradation or interruption in availability of information already existing in cyber risk dashboards used daily.

How long is the transition period?

The transition period has been extended until January 2nd while the DIR and SDL teams work to ensure that all data repositories are available in the SDL environment with the most up to date information available. After January 2nd, the legacy dashboards will no longer be available and all cyber risk dashboards will be based in the SDL. Please refer to the infographic below for a summary of the current status and timelines!

Have more questions? Reach out to the team!

Please reach out with questions or for assistance:
Slack: #cyber-risk-management
Email: CRMPMO@cms.hhs.gov



Monday, November 20, 2023

Now in PRODUCTION

Security data Lake

45-day Transition starts now

What's Happening?

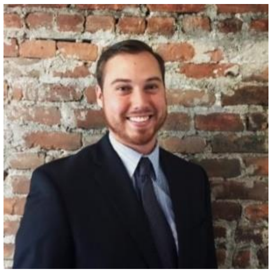
The SDL is live and in Production,
the Core CRM Dashboards are now available!

Core CRM dashboards

- Ongoing Authorization (OA)
- Vulnerability Monitoring (VUL)
- Master Device Record (MDR)
- Known Exploited Vulnerabilities (KEV)
- Vulnerability Related Asset Details
- Dynamic Cyber Risk Management Reports

how to get help & Report issues

Please contact the CRM PMO mailbox at crmpmo@cms.hhs.gov or reach out via the #cyber-risk-management Slack channel. In addition, you will see regularly scheduled weekly "CRM Open House – SDL Production" sessions, which are opportunities to speak with SMEs for any questions, concerns, or feedback.



Jonathan Herrick is a Senior Project Manager for ECS; he works in the project management office (PMO) supporting the Division of Implementation & Reporting within the Information Security & Privacy Group and Office of Information Technology. In his role, Jonathan helps to manage and coordinate projects, develop and lead communications, and support the Cyber Risk Management Program at CMS.

Cybersecurity Community Forum Notes from September, October, and November 2023

Cole Schenck (Assyst)

In September 2023:

- Omar Nolan gave some updates regarding CFACTS, SDL, new generation dashboards and reporting, and data quality.
- Jay Shao wanted some feedback on a survey ISPG is running about experiences with tabletop exercises. You can find the survey here

In October 2023:

- Elizabeth Schweinsberg held a Zero Trust poll during the forum to get a better understanding of what teams are already doing with encryption key management. With the results, she wants to publish additional guidance to go along with the Key Management Program Manual from ISPG.
- Josh Meagher gave a demonstration of the recently launched Computer-Based Training and Learning Management System. He walked us through the different parts of the dashboard and explained what every part does.

In November 2023:

- Erica Rebstock and Daniel Bowne gave a presentation on SaaS Governance They explained what SaaS Governance entails and the challenges faced using SaaS applications. The proposed Rapid Cloud Review (RCR) as a solution as well as alerting the group to additions to IS2P2 Policy (CMS-CLD-1 and CMS-CLD-1.1). They continued by teaching us about the Discovery pillar of the SaaS Governance Framework. This pillar encapsulates asset management, security, unaccredited SaaS, SaaS inventory, and more. They also listed tools and techniques for implementing SaaS Discovery and the challenges faced doing so.
- Elizabeth Schweinsberg announced the Zero Trust team is working with the Security Data Lake team to build a dashboard where people can look up the zero trust maturity levels of their physical system in 2024. She also walked us through how to update identity management systems in CFACTS. Furthermore, she talked about different projects the Zero Trust team is working on including identity projects, device projects, networks projects, and more.

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 September and November 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 September meeting, Derek Bailey wanted to know other ISSOs' experience with ACT teams. He explained that teams will vary on what tier 2 artefacts they want or will accept. Other members of the CISAB shared their concerns as well. Bobin Rajan shared how his team would prepare for assessments by creating action plans that some assessors wouldn't accept. Jason Ashbaugh that creating contingency plans during an ACT was more for compliance rather than usage during a real emergency. The cohort agreed there should be clear requirements as to what is needed in each ACT report as well as desired outcomes. For our second topic, Kevin Allen Dorsey wanted to ask the cohort how useful they found tabletop exercises. Jason Ashbaugh believes functional tests are valuable but aren't sufficient to auditors. Derek Bailey encourages his teams to do VR exercises because he believes it's more useful that talking through a contingency plan and checking off boxes. The cohort agreed tabletop exercises are useful but there isn't a defined expectation or outcome by completing them. For our final topic, Derek Bailey wanted the cohort's thoughts about Microsoft's new Copilot product, an AI tool designed to help the user. He wanted to know where that data was going or whether or not the user had full control of their data.

In our November meeting, Zil Zukhruf Sheikh wanted a place for stakeholders to be able to introduce themselves and explain to the cohort the projects they're working on. Casey Douglas invited the Governance, Risk, and Compliance team to explain what their team is currently working on, but they were unable to attend. Casey Douglas explained that the GRC team was working on something called the RACI Matrix but wasn't able to elaborate further. For our second topic, Benjamin Ohe wanted to talk more about hardened container images. He realized quite a few teams at CMS are utilizing them but seem to be struggling with vulnerabilities as well as broken container images. Evan Woodward, from the Bat Cave project, noticed a similar pattern and suggested ADO's use Alpine as a base image since it had a very small attack surface. The cohort agreed there should be baseline documentation in place to combat container image vulnerabilities. For our final topic, Casey Douglas wanted to know if CISA was in talks to revise BOD 19-02 to include the updated CVSS. Furthermore, her team was experiencing difficulties with the Tenable dashboard not displaying KEVs. Keith Busby and Michael Kania were present to help answer questions in regard to the Tenable dashboard. If any of the topics discussed here sounded 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 January CISAB meeting will be held January 31st 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