CMS

ISSO Journal

...by and for CMS Cybersecurity Professionals

Spring 2021

Issue 16

CMS ISSO JOURNAL

Spring 2021 Issue 16

Highlights

FEATURE STORIES

3
Protect Your Most Critical Data With Trustwave's DbProtect Vulnerability Management Scanner
Aaron Burnett, Steven Robbins, and Toan Luong

UPDATES

5
Data Guardian Update - *Eric Larson, IRIS Health Solutions, LLC*

10
ISPG Knowledge Management Portal Update - *Doug Nock, ISPG*

11
CMS Security and Privacy Publication Update – *Clarence Mayfield, ISPG*

12
Training Update

14
ISSO Forum Notes
John Myers

EDUCATION AND TRAINING UPDATES

9
Upcoming Splunk Events & Training Available to You

10
Free SANS Conferences

The *CMS ISSO Journal* seeks to 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.

Along with professional knowledge exchange, the Journal serves as a companion to the CMS ISSO Forum in fostering communications within the ISSO Community and imparting information from ISPG and OIT leadership.

If you would like to submit an article or have any questions or comments, email us at isso@cms.hhs.gov, Slack #cms-isso. Don.Bartley@cms.hhs.gov or John.Myers2@cms.hhs.gov.

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

Journal Contents

Protect Your Most Critical Data with Trustwave's DbProtect Vulnerability Management Scanner - *Aaron Burnett, Steven Robbins, and Toan Luong CMS ISPG DCTSO* 3

Data Guardian Update - *Eric Larson, IRIS Health Solutions, LLC* 5

BATCave Initiative – *Rob Wood, Chief Information Security Officer* 6

Office of Enterprise Data & Analytics, Data Use Agreement Overview – *Andrea Triggs and Tom Latella* 7

Beneficiary Data Protection Initiative/Phishing Program Enhancement - *Kim Hemby & Alisa Sheppard* 8

Cyber Hall of Fame 9

Education Update- Upcoming Splunk Events & Training Available to You 9

ISPG Knowledge Management Portal Update - *Doug Nock, ISPG* 10

Education Update – Free SANS Conferences 10

CMS Security and Privacy Publication Update – *Clarence Mayfield, ISPG* 11

Training Update 12

Just Released! Cybersecurity and Privacy Audit Video 12

Role Based Training (RBT) -- Delivered Right to You! 12

Customer Centric Cybersecurity 13

Opportunity is Knocking 13

Catch of the Month 13

ISSO Forum Notes for April, May and June 2021 13

Internal and External Resources for ISSOs 14

Protect Your Most Critical Data with Trustwave's DbProtect Vulnerability Management Scanner - *Aaron Burnett, Steven Robbins, and Toan Luong CMS ISPG DCTSO*

Databases and large data stores often hold the most mission critical data within CMS to include protected health information (PHI), personally identifiable information (PII), and federal tax information (FTI). Trustwave's DbProtect database scanner enables CMS Information System Security Officer's (ISSO) to quickly identify known vulnerabilities and misconfigurations and helps reduce the threat of a data breach for both on premise and cloud-based systems.

Enterprise Database Management Systems (DBMS) and large data stores contain CMS' most valuable mission critical data making them prized targets for cybercriminals and nation states. CMS is responsible for safeguarding the nation's largest collection of PII, PHI, FTI, provider and beneficiary information, and intellectual property. According to Cybersecurity Ventures, "data breaches and other cybercrime damages are projected to reach $6 trillion in 2021". Cyber-attacks against Healthcare organizations have increased by 12.1% since the beginning of the year.[1]

Spider Labs (TW) identified the Top Database Security Challenges that large enterprises need to be mindful of while assessing DB risk. Trustwave's DbProtect: Vulnerability Management (VM) module enables CMS ISSOs to address the following challenges: excessive privileges, missing patches, poor audit trail, password management, and cloud adoption. DbProtect also provides additional capability modules that address a more comprehensive list of DB security challenges.

Top Database Security Challenges

- Excessive Privileges
- Privilege Abuse
- Privilege Escalation
- Missing Patches
- SQL Injection
- Poor Audit Trail
- Poor Password Management
- Cloud Adoption
- Insider Threat
- Account Compromise

DbProtect is also capable of providing continuous monitoring of enterprise DB and large data stores with scheduled scanning and can be leveraged as a key risk information source (RIS) to support Ongoing Authorization (OA). DbProtect VM module is capable of scanning and reporting against the following Acceptable Risk Safeguards (ARS) 3.1 control families:

[1] Source: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

- Access Control
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Identification and Authentication
- Risk Assessment
- System and Information Integrity

Scan reports provide CMS ISSO's and auditors with database health reports which are used to help inform risk-based decisions for system authorizations. The scan policies are consistent with the DISA STIG and CIS Benchmark policies that are currently used by the CMS Adaptive Capabilities Testing (ACT) assessment teams. Routine scanning, led by the CMS Cybersecurity Integration Center (CCIC) Vulnerability Assessment Team (VAT), replaces the existing manual SQL collection scripts run by DBAs and ensures active compliance.

The ability to fully automate DB scans and reporting provides ISSO's with real time situational awareness across multiple DB platforms and ensures CMS systems are consistently scanned with the latest federal guidelines and best practices. By having this information available throughout the information system lifecycle between formal assessments, it provides ISSO's a more thorough understanding of DB configuration and control. This removes unexpected surprises when the audit team reviews and evaluates the controls and their implementation. DbProtect reports vary from high level executive dashboards, to detailed findings reports for ISSOs and DBAs. Findings reports support drill down capabilities down to specific occurrences and recommended mitigations.

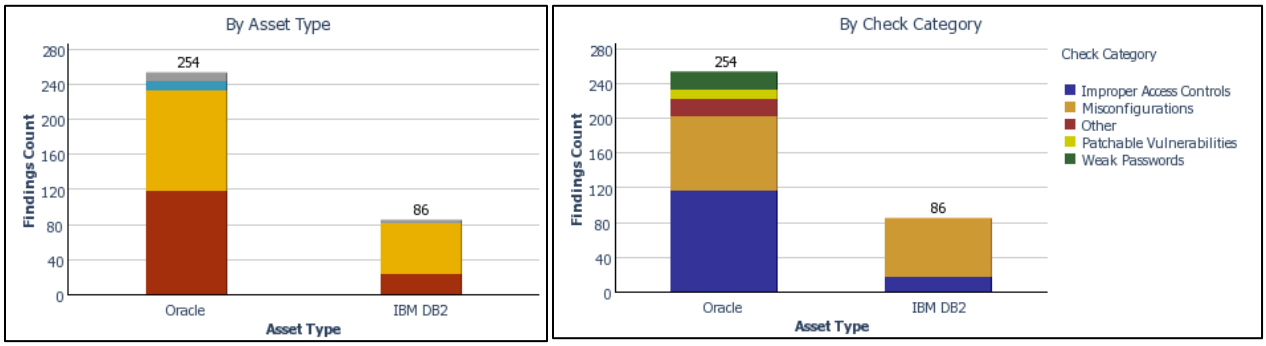

Figure 1. Risk Position by Asset and Check Category

The DbProtect Implementation team has successfully scanned 60+ DB instances across the CMS lower environments, PROD, and AWS. Scans spanned across 5 DB platforms which resulted in the identification of dozens of validated findings by the DBA teams. Scans are typically completed in less than 5 minutes and performance degradation has been minimal. The CMS Adaptive Capabilities Testing (ACT) team is currently leveraging DbProtect scan reports in support of system authorization decisions.

DbProtect currently supports the follow database platforms and large data stores:

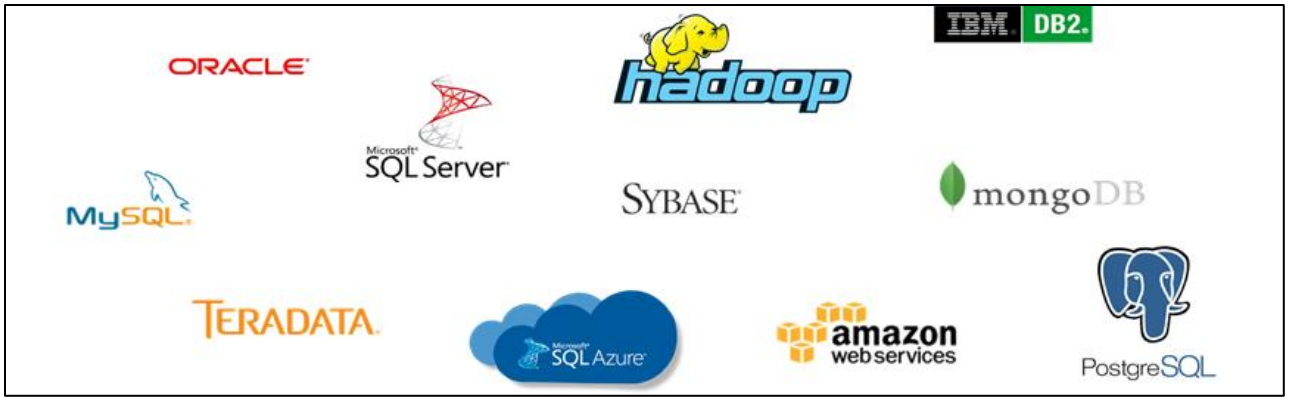

Figure 2: DbProtect supported platforms

DbProtect is intended to work in conjunction with existing CMS database security validation capabilities including the CMS Security Automation Framework (SAF) Inspec database security validation profiles. DbProtect and InSpec both provide security compliance checks; an analysis of report findings indicate they are best used together to provide a comprehensive picture of DB vulnerabilities and risk.

The CMS SAF team also created a converter in Heimdall tools to visualize DbProtect scan results in Heimdall to provide a comprehensive visual across multiple types of compliance checks. In addition to VM scanning, DbProtect is capable of supporting User Rights Review and Activity Monitoring at the DB level to provide an additional layer of protection.

Please contact the DbProtect Federal Lead Aaron Burnett for more information (Aaron.Burnett@cms.hhs.gov).

Data Guardian Update - *Eric Larson, IRIS Health Solutions, LLC*

The Data Guardian Program was created to implement CMS's Beneficiary Data Protection Initiative (BDPI). Its focus is to address organizational security/privacy issues, ensuring a coordinated and consistent approach to safeguarding CMS data, including Personally Identifiable Information (PII) and Protected Health Information (PHI). The aim is to enhance and promote good cyber hygiene across the CMS enterprise. The Data Guardians meet on the third Wednesday of each month and discussions cover a range of cyber hygiene do's and don'ts, along with current cyber events and emerging policies and technologies. The information below contains a list of topics that summarize recent discussions during these Data Guardian meetings.

Attention ISSOs

- A reminder to all ISSOs – You must submit your Self-Assessment and SCA CAAT files to the CISO Mailbox after every assessment.
- The Import Control Implementation Details application is now available in CFACTS for ISSOs and ISSO Contractor Support to bulk update the private/shared control implementation details.
    - Please watch the video "**How to upload Implementation details**" available in the CFACTS welcome page before using this application.
    - A how to guide is also added under section 11.6 of CFACTS User Manual.
- For further questions please reach out to the CISO team at ciso@cms.hhs.gov

BATCave Initiative – *Rob Wood, Chief Information Security Officer*

Rob introduced the upcoming project called, the "BATCave Initiative" with a continuous authorization and verification engine. Rob has introduced this concept because of the many challenges currently faced when introducing new software, products, and technology into the CMS ecosystems. Within federal systems, there are currently many processes involved in governance, risk management, and compliance requirements including policies and required security and privacy checks. In addition, within CMS, there is an average window of 540-800 hours spent on completing the ATO process as well as ongoing maintenance and annual updates. The BATCave Initiative is designed to reduce the level of effort and time it takes to complete the ATO process by compartmentalizing the workflow process and changing and streamlining what needs to be done. In addition, the general belief is that the current ATO process is not making CMS systems safer or more secure but provides a layer of accountability and proof that something was done for the auditors.

Adding to the challenges above are the government's efforts to move to the Cloud over the past few years. There are now hundreds of connections to the cloud from CMS in a dynamic space where the infrastructure is rarely reused or is passed on in a less than ideal state to be used, which causes a lot of overhead and increased cost.

Project Goals are to Develop Performance and Continuous Security and Privacy Monitoring

a) Develop Performance - The idea is to optimize and encourage software and system developer performance. As an example, a business owner identifies a problem. The team then comes up with an idea on how to solve the problem, which leads to something running in production trying to solve that problem faster. The proposed objective is to reduce the typical development and change time, which could potentially take years to complete.

b) Continuous Security and Privacy Monitoring – Secondly, we are the Information Security and Privacy Group. Consequently, we need to move to a model which provides safer and more secure information systems because the current snapshot view into our security landscape does not cut it in today's world. We want continuous security (and privacy) monitoring and not just points in time. We want to be able to infer the security properties of anything running in the CMS ecosystem at any time, especially on the heels of the new executive order that came out last week where there is a huge emphasis on making sure that trusted resilient systems are running in production handling the nation's problems. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

This requires doing something different because ISPG in general as well as CMS as an agency, does not have the resources to support special snowflake development across the sprawling CMS ecosystem. Therefore, we are marching towards a more formalized adoption of DevSecOps (unification of development, security, and operations work; see definition below), minimizing security friction, incentivizing more change, and shifting from point-in-time to continuous security monitoring by embracing agile delivery schedule/cadence, vs. delivering software releases on an annual fix cadence. This operating model will allow people to deploy as often as they want or need to without the typical roadblocks.

The BATCave initiative is modeled after the Air Force's, *Platform One,* and is a fully managed suite of DevSecOps tools geared towards faster product delivery and, in our case, we are focusing on ATOs. As with any new process, some concepts should be defined.

c) DevSecOps – The integration of security into emerging agile IT and DevOps development, as seamlessly and as transparent as possible on an ongoing basis. Ideally, this methodology breaks projects into smaller chunks without reducing the agility or speed of development.
d) Containers – An immutable, packaged piece of an application that contains everything needed to run.
e) Kubernetes – An open-source runtime environment to manage containerized workloads and services.

Kubernetes, which came out of Google in 2014, is an open-source project that acts as an orchestrator tool for managing the containers. For example, MS word is an application. It needs CPU, an operating system, and Windows or Mac. It needs networking, storage to store files, CPU, and RAM to load and run. There needs to be some kind of logic built into the actual Word program itself. CMS has the same issues with our applications. Therefore, a container is trying to take the minimum (x) that an application needs to run and bundle it together into different modular chunks that make a program application run and they can be layered. If change is needed, it is done at the container level.

Office of Enterprise Data & Analytics, Data Use Agreement Overview –

Andrea Triggs and Tom Latella

Tom and Andrea introduced themselves to the group and explained that a DUA is a HIPPA required agreement between CMS and a requesting organization. It establishes permitted uses and disclosures of limited data sets (LDSs) that usually contain protected health information (PHI) and/or personally identifiable information (PII) for a specific project or study. CMS enters into DUAs with data requesters / researchers to ensure that they adhere to CMS privacy and security requirements and data release policies.

The DUA identifies who may use or receive the information and prohibits the recipient from using or further disclosing the information, except as permitted by the agreement or as permitted by law. It is active for one year and is project and type-specific which means that you must know if the requesting organization is coming in as a contractor or specific researcher to perform the study.

The DUA form must be reviewed, approved, and placed in CMS Enterprise Privacy Policy Engine (EPPE) system by the DUA team before the release of the data. Based on the security and privacy best practice of "Least Privileged", only the minimum data necessary to accomplish the study will be provided. This is an agency-specific legal, privacy, and security requirement because CMS does get audited. In addition, since CMS is the custodian of Medicare beneficiary data, the beneficiaries have a right to know how their data is being maintained and the reason/purpose it is distributed outside of CMS to external entities. Consequently, we also have obligations to our beneficiaries.

A DUA must have a Requestor and only one Requestor and at least one Custodian. The difference is that there can be more than one Custodian on a DUA. The Requester role legally binds the organization to the agreement while the Custodian role safeguards, handles, and controls access.

There are six different types of DUAs

- Contractor – a CMS Contractor doing work on behalf of CMS. Most DUA's fall under Research
- Researcher – Limited Data Set (LDS) – LDSs do not have direct identifiers within the data, like the full birth date or date of the procedure. It might only have a Month and Year of birth. In addition, the difference between an LDS, Research Identifiable Files (RIF), or Contractor is that the LDS is a limited data set requiring

less paperwork and is a faster process. So, if an organization can do their research with an LDS that is the way to go. In addition, LDS is less expensive than the research identifiable files.

- Researcher – Research Identifiable Files (RIF) – Data that includes identifiable PII and PHI. The processing for RIFs requires more paperwork, more processing time, and is more expensive than the LDS process.
- Non-DUA Tracking – These do not fall under the one-year limit as the other DUAs above. A DUA is a form that has terms and conditions. Sometimes, those terms and conditions do not apply to oversight agencies, court orders, and CMMI models getting the data for healthcare operations for routine use only; they do not have to comply with the terms and conditions within the actual form. That is why it is called Non-DUA tracking. However, we still are required to track their use, but with maybe a different form.
- Oversight Agencies - Requires completion of a different form
- Court Orders - When Court Order DUAs are received, we review the DUA to make sure it is complete. It is then forwarded over to the Privacy team for review and approval. Once approved, it is sent back to the DUA team for processing.

Finally, we track the DUAs in our Enterprise Privacy Policy Engine (EPPE) Tracking System that was implemented to replace the manual labor-intensive process of tracking DUAs via the DUA mailbox. EPPE has a self-service feature so that Contractors and Researchers are required to input requests directly into EPPE. Also, we continue to track every email that comes into the DUA mailbox, datauseagreement@cms.hhs.gov

For more information on agreements, including Computer Matching Agreements (CMAs), Data Use Agreements (DUAs), Information Exchange Agreements (IEAs), System of Record Notices (SORNs), and Third-Party Website & Application (TPWA)) see this link: CMS Privacy Home Page

Beneficiary Data Protection Initiative/Phishing Program Enhancement - *Kim Hemby & Alisa Sheppard*

Kim notified the group that she has been selected for detail at HHS to manage their component Data Guardian Training program. Alisa Sheppard will backfill her duties.

To inform the CMS community on the role of the Data Guardian's, we created a quick introductory video that can be found when you sign into the CMS Computer Based Training site: https://www.cms.gov/CBT/login/default.aspx?ReturnUrl=%2fcbt%2fForms%2fRBTraining.aspx

We sent two phishing training campaigns: one on April 6 and the second on May 17. The first was titled: "Activate Zoom Account" and was distributed to 10,374 accounts with the following results:

- The number who reported the phish to the SOC – 3221 (The goal is to double this number once everyone receives the Report Phishing icon on his or her Outlook ribbon).
- Opened Email Only – 527
- Clicked on the link but did not submit data – 74
- Clicked on the link and submitted CMS credentials – 87

The second campaign in May was titled, "Message from Your Childs School" and was distributed to 10,414 accounts with the following results:

- The number who reported the phish to the SOC – 3,458
- Opened Email Only – 2,548
- Clicked on the link but did not submit data – 142.
- Clicked on the link and submitted child's google credentials – 30.

Mike Pagels reinforced to the group that the phishing program is designed to identify teachable moments with an emphasis on training to reduce the likelihood that a staff member would click on a real-world phishing attempt. Phishing is the number one way that bad actors can access our systems. Consequently, we need everyone to be educated (including the educators) on how to identify a phishing email.

Lastly, Lee Moore with the CMS Security Operation Center explained that CMS is piloting a Credential phishing prevention software solution. It is a Palo Alto product that detects and prevents in-progress phishing attacks, which prevents credential theft, by controlling sites where users can submit corporate credentials based on the site's URL category. This allows you to block users from submitting credentials to untrusted sites while allowing them to continue to submit credentials to known and approved sites.

Cyber Hall of Fame

The CMS Cyber Hall of Fame was created to recognize those individuals on the "front lines" who have demonstrated their commitment to keeping our data, systems, and networks safe by preventing actual phishing attacks. Since January 1, 2021, CMS staff reported 114 real-world phishing attempts! You can access the Cyber Hall of Fame via the Beneficiary Data Protection initiative website at https://cmsintranet.share.cms.gov/CT/Pages/BeneficiaryDataProtectionInitiative.aspx.

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

Education Update

Upcoming Splunk Events & Training Available to You

You are invited to our upcoming events and free training

Upcoming Workshops:

- Infrastructure Monitoring & Troubleshooting (IMT) Workshop on 6/9
- Splunk 4 Rookies Workshop on 6/17
- Business Service Insights Workshop on 6/23

There is no cost for the following courses when using your CMS email address.

Free Instructor On Demand Courses:

- Splunk Fundamentals Part 1
- Splunk Fundamentals Part 2
- Splunk Fundamentals Part 3
- Advanced Searching & Reporting with Splunk
- Creating Dashboards with Splunk

If you have any questions, please don't hesitate to reach out! Tallie Dameron, Splunk > Federal Civilian O: (703) 206-6596 | M: (423) 360-2230 Email: TDameron@splunk.com

ISPG Knowledge Management Portal Update - *Doug Nock, ISPG*

Customer Voices Influencing New Product Developments

At the end of April, ISPG conducted its first virtual "human-centered" design sprint with a small cohort of CMS customers, which included ISSOs, data guardians, Cyber Risk Advisors, auditors, vendors, business and system owners. The design sprint was held to help inform the development of a new knowledge management portal site, that will eventually serve as a single authoritative source for all your security & privacy related needs. Typically, design sprints are face-to-face events that are a week in duration. With the help of Team Sprezzatura, ISPG's PMO contractor, the process was streamlined so the work could be done virtually in a fraction of the time.

Leslie Nettles, who serves as the portal product owner, said "this has been a passion project for me for quite some time. After spending many years supporting the CISO and Privacy mailbox resources, I wanted to create a more meaningful experience for those customers who need our information to do their jobs. The design sprint gave me an opportunity to step into the 'shoes of our customers' and really understand their needs. I feel confident that this time investment with our customers will allow me to develop a site that they will want to visit again and again, and improve our security posture across the agency."

ISPG is hoping to complete the first release of the knowledge management portal by the end of the summer. Additional releases are planned that will give customers access to the most frequently asked questions, a robust search engine, a virtual agent/online chat resource, and reformatted handbooks/manuals that are geared to specific customer roles and competency levels. The portal will also cater to ISPG's multi-generational workforce and their needs, where information will be provided using infographics and video technology. - *Doug Nock, ISPG*

Education Update – Free SANS Conferences

- SANS is offering ALL of their 2021 summits for free. Please see below. As always, supervisory approval is needed. Also, don't forget that we have plenty of funding for actual SANS classes (federal employees only). Please visit the SANS SharePoint page for more info: https://share.cms.gov/Office/OIT/ISPG/SitePages/SANS%20Training%20Information%20Page.aspx
- Register interest for upcoming Summits and we'll notify you when registration opens:
  - DFIR Summit | July 22-23
  - Security Awareness Summit | August 5-6
  - Cybersecurity Leadership Summit | August 20
  - Cyber Defense Summit | September 9-10
  - Threat Hunting Summit | October 7-8
  - Cloud & DevOps Security 2021 + Summit @Night | October 18-23
  - Pen Test HackFest Summit | November 11-12

Contact Norman Brown for more information 301-254-6255 or Norman.Brown@cms.hhs.gov

CMS Security and Privacy Publication Update – *Clarence Mayfield, ISPG*

The ISPG Policy Team has been busy in these past few months working on a number of projects to ensure our stakeholders have the tools needed to make decisions that improve the security posture of their environment. These projects include:

- Biweekly discussion with stakeholders (ISSOs, IT Managers, Developers etc..) on the ARS 5.0 and the impact on CMS systems
- Developed a Confluence page for the following
    - ARS 5.0
    - Digital Identity

Implemented Really Simple Syndication on the Information Security and Privacy Library. See the link below:

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

Updated the following Risk Management Handbooks and associated guidance:

- RMH Chapter 14 Risk Assessment – (Updated HVA Guidance (CISA and RVA requirements, and Vulnerability Remediation Timelines)
- RMH Chapter 6 Contingency Planning (Reflect the System BIA per NIST 800-34 Rev 1)
    - NIST BIA System Template NIST 800-34 Rev 1 (As a component of the ISCP it is added for *Prioritizing systems based on their Mission Business*)
- RMH Chapter 12 Planning – (Added a procedure for the ATO Letter submission to the FedRAMP PMO Memo)

Implemented the following Policy and Memorandums:

- Vulnerability Disclosure Policy Update (updated the policy to provide guidance for researchers to report vulnerabilities which impact the CMS environment without fear of recourse)
- CISO Memorandum 21-01 – Best Practices and Guidelines for the use CMS Approved Collaboration Tools (March 30, 2021)
- CIO Memorandum: CMS Strategy for Encrypting Sensitive Information
- System Retirement Memo (Updated to reflect Robert Wood, as the new Chief Information Security Officer (CISO)
- CISO Memorandum: Keeping CMS CyberSafe with Deception-based Technology (April 13, 2021)

To avoid the use of offensive language which may be implied as either sexist, racist, or showing bias, prejudice or denigrating to a particular group of people, ISPG has begun updating its documentation to be more inclusive. As a part of this effort ISPG has updating the following documents and will continue to perform its task on all of its documents.

- POAM Process Guide

- RMH Chapter 8 Incident Response
- RMH Chapter 11 Physical and Environmental Protection
- RMH Chapter 5 Configuration Management

We are working on two documents the CMS Acceptable Risk Safeguards (ARS) 5.0 and the CMS Information Systems Security and Privacy Policy (IS2P2). It is our intent to release the documents by the fall. These documents will be the foundation by which CMS will implement security and privacy requirements within the CMS environment.

- The IS2P2 is a supplement to the HHS IS2P as it will be CMS specific and provide additional policy guidance of how we implement our Security and Privacy Program.
- The ARS will incorporate the HHS Standards and the CMS specific standards as required to ensure we manage risk in a manner which is appropriate to the CMS environment

Through the implementation of these two documents we expect to embrace technology and work with our stakeholders to manage the risks associated. This includes maximizing the services associated and allowing the technology to be used as it was designed to support our stakeholders.

*Note – *Upon publishing ARS 5.0 it is highly recommended that systems perform an assessment to determine any control implementations that do not meet the ARS 5.0 requirements. It is expected that after one (1) year a comprehensive assessment will be completed and the systems will be in compliance with the ARS 5.0 control implementation.*

Please contact the CISO Mailbox for any questions, or you may reach us on Slack.

Clarence Mayfield is a Security and Privacy Subject Matter Expert in Information Security and Privacy Group.

Training Update

This content originally appeared in "This Just In" for June 2021.

Just Released! Cybersecurity and Privacy Audit Video

Cybersecurity and privacy audits are crucial to the success of CMS operations, but are sometimes misunderstood. Ever wonder what these audits are all about? This informative and enjoyable animated video covers the basics of Cybersecurity and Privacy Audits. If you have any feedback or questions about this video, please contact the Audit Team. Don't delay -- watch it today!

Role Based Training (RBT) -- Delivered Right to You!

CMS employees with Significant Security and Privacy Responsibilities (SSR) need to complete their specialized role-based training on an annual basis. Completing the training is simple and easy. All you have to do is log in to CBT and complete the training assigned to you based on your role. Have any questions? Meet with your manager to discuss your SSR role and related training. Or visit the CMS RBT Training page for more helpful information.

Customer Centric Cybersecurity

Cybersecurity and privacy protection is all about people, which is why ISPG's new product development is all about Human-centered Design (HCD). HCD focuses on user-friendly solutions. In collaboration with customers across CMS, ISPG is creating a new information and resource portal. Following HCD principles, the new portal begins with customer needs, requirements and preferences. ISPG's Leslie Nettles explains, "HCD gives us the opportunity to step into the shoes of our customers. It allows us to really understand and meet their needs, while simultaneously serving to improve our security posture across the agency." Stay tuned for more HCD updates from ISPG!

Opportunity is Knocking

Are you interested in a work detail? ISPG is looking for a training task area lead. Contact Shawnte Singletary for more information.

CMS CYBERWORKS - Save the Date! July 21, 2021

Mark your calendars: the Information Security & Privacy Group (ISPG) will host CMS CYBERWORKS in July. Creating a culture of cybersecurity is critical for all organizations, including CMS. The internet is used to support many of our day-to-day activities and for many purposes. As technology improves, there is evidence that cyber-attacks are occurring more frequently and if they are successful, their impacts can be damaging. Knowing how to identify and prevent common cyber-attacks helps promotes a more secure internet environment for everyone. Our goal for CYBERWORKS is to engage cyber and privacy professionals in discussions focused on cybersecurity and privacy priorities, trends, improvements, and ways to confront unparalleled security challenges!

Catch of the Month

Thank you to all Phishing Hall of Fame inductees. Since January 2021, 95 vigilant CMS staff have identified and reported malicious "phishing" scams. When in doubt, phish it out!

ISPG Training Team

ISSO Forum Notes for April, May and June 2021

On April 6, 2021 there were two major presentations.

- John Rudolph provided an overview of **Supply Chain Risk Management**.
- Rob Wood talked about **Certified Pipelines and How They May Tie into Ongoing Authorization.**

On May 11, 2021 there were two major presentations.

- Dennis Hazelwood from DSI presented on **CMS Policy and Procedure for Requesting to Perform Work Outside the United States and its Territories**.
- Rob Wood discussed the **CMS Enterprise Kubernetes Buildout.**

On June 8, 2021 there were three major presentations.

- **Nicholas Wojnowski**, **Jennifer Clark** and **Kyle Latz** demonstrated updated features in CFACTS.
- **Antoinette Johnson** discussed changes in the Technical Review Board concept of operations and features.
- **Rob Wood** discussed AWS Security Hub rollout for CMS systems.

Find a complete version of the slides and the transcripts for these and other forums at 2021 Forum Materials - ISPG ISSO Program. (Requires Confluence access).

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

ISSO SharePoint Site at https://share.cms.gov/Office/OIT/ISPG/DSPC/ISPG%20DSPC%20ISSO%20Library/Forms/AllItems.aspx

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