CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

What's New in ISPG 2025

Leslie Nettles

CSCOUT
January 28, 2025

Hot Topics

- Vetting and Credentialing
- Bug Bounty
- Red Team Exercises
- RMF Updates in CFACTS and CyberGeek

Vetting & Credentialing

- CMS is taking a proactive stance to further secure its information and information systems. A key step is ensuring all contractors go through appropriate vetting (background checks) and credentialing (PIV or other MFA).
  - Enabling PIV and PR-MFA
  - Ensure we have an understanding of who is accessing our information
- ISPG is working with other parts of CMS to improve our vetting and credentialling coverage
- CMS is getting ready to flow all contractors through the process, and is working on:

  Time: improving the time it takes a contractor to get their paperwork and fingerprints submitted and reviewed (e.g., vetting)
  - Access to Credentials: working through PIV delivery and access to alternate MFA. PIV cards are hard to get if the contractor is far from the office or will not be coming to the office
  - Scope: ensuring all contractors are assessed; currently, not every contractor goes through vetting and different MACs have different vetting coverage

Vetting & Credentialling

In 2024, OIT made the following steps to improve vetting and credentialling:

- Contractor Access Data Call to inventory who is on which contracts
  - Thank you to all who participated, especially your CORS!
- Addition of the Contract Roster to ICT (plus other changes to ICT)
  - That way we don't have to do that data call again
- Research and development of other "credentialling" options
  - FIDO2 and WebAuthn top the list for phishing-resistant MFA
  - Exploring alternate ways of distributing PIV certificates
- Identification of ways to improve the ICT application process

Vetting & Credentialling-Continued

In 2025, you'll see more changes throughout CMS:

- Forthcoming memo on phishing-resistant MFA expectations for FISMA systems
  - All FISMA systems for providers must offer a phishing-resistant MFA option by September 2026
- Enforcement of finishing vetting in a timely manner to maintain EUA access
- Improvements to vetting systems to reduce submission errors
  - And faster processing by Badging
- Options to use FIDO2 and WebAuthn along side PIV cards in IDM and other authentication systems

What is Bug Bounty

What: Organizations provide financial incentives (“bounties”) for researchers to discover vulnerabilities (“bugs”) in public facing sites.

How: Programs base bounty rewards on the severity of vulnerabilities, and rewards increase as the potential impact increases.

Who: 3rd party organizations recruit vetted participants through their platform (i.e. BugCrowd)

Why: Provides a way for organizations to improve their applications’ security **after** public release. Expert bounty hunters will likely ignore free programs. Without an incentive to report vulnerabilities to CMS directly, hackers can make more money disclosing this information on the dark web.

CMS Bug Bounty Journey

- Moved from HHS Vulnerability Disclosure Program to CISA's Program
  - CMS had received 0 submissions in ~9 months in 2023 with the HHS program
- Movement to CISA's VDP was a requirement if CMS wanted to take advantage of CISA's Bug Bounty Program.
- Time and Resource Allocation:
  - **Prep Time:** 4 months (July-Oct)
  - **Cost:** $75,000 (CISA covered an addition $75K of admin costs)
  - **Program Time:** Estimated 4-6 weeks
  - **People:** ~11 (5 CMS, 3 CISA, 3 Vendor)
  - **Results:**
    - 134 Submissions received
    - 87 Accepted
    - 12 Resolved

Bug Bounty Results

We allocated $75,000 to spend over 6 weeks

We spent $66,500 in 4 days……

Bug Bounty Conclusions

- Bug Bounties are an extremely cost-effective way to find vulnerabilities in your systems

- CMS will host another bug bounty in January 2025 with a bounty pool of $100k, including new targets, and investigate making bug bounties regular piece of our proactive security strategy going forward

What is a Red Team Exercise?

- An exercise, reflecting real-world conditions that is conducted as a simulated adversarial attempt to compromise organizational missions or business processes and to provide a comprehensive assessment of the security capabilities of an organization and its systems.
- The red team's goals are to:
  - Show the effects of a successful attack
  - Demonstrate what works for the defenders, also known as the blue team
  - Identify and assess vulnerabilities
  - Test assumptions
  - Reveal security risks and limitations

Who must have a Red Team Exercise?

All CMS systems that meet the following criteria must undergo Red Team activities at least once during their ATO cycle:

- **Public-Facing Systems:** Systems accessible from outside the CMS network.
- **Handling PII:** Systems that process, store, or transmit PII.
- **Cloud-Hosted:** Systems hosted in the cloud.
- **Not Exclusively SaaS:** Systems that are not purely SaaS solutions.

Requirements for Red Team Exercises

Scope: Red Team assessments must cover all relevant components, including network, application.

Frequency: Red Team activities must be conducted at least once during each ATO cycle.

Reporting: Detailed reports of Red Team findings and remediation actions must be submitted to the Information Security and Privacy Group (ISPG) within 30 days of the assessment completion.

Coordination: Red Team activities must be coordinated with system owners and relevant stakeholders to minimize operational disruptions.

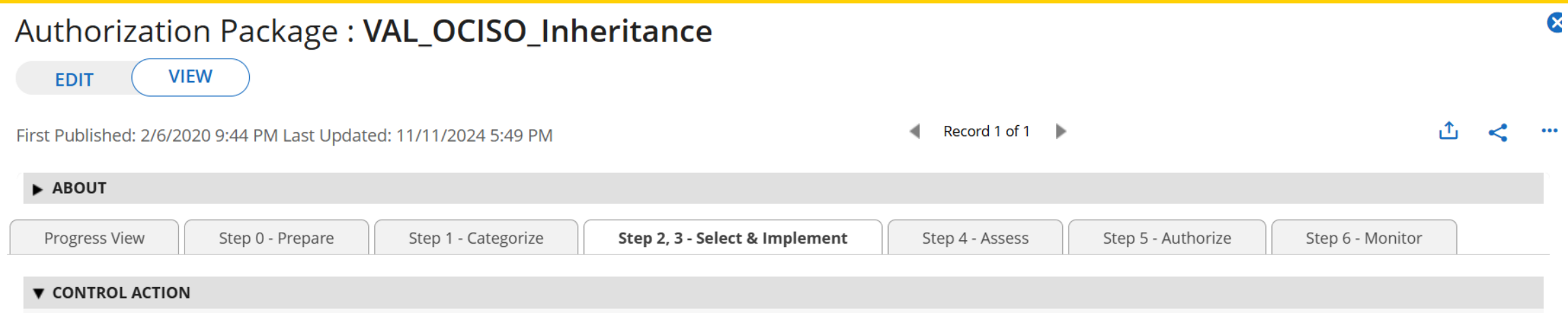
Red Team Exercise Next Steps

- OIT is reviewing a memo from the CISO regarding implementation of Red Team Exercise requirements.
- Once approved, targeted communications will be completed to the systems that have been identified as meeting the requirements.
- 90 days after the memo is signed, ARS security control CA-08(02) will be applied to applicable systems.

Risk Management Framework: CFACTS and CyberGeek

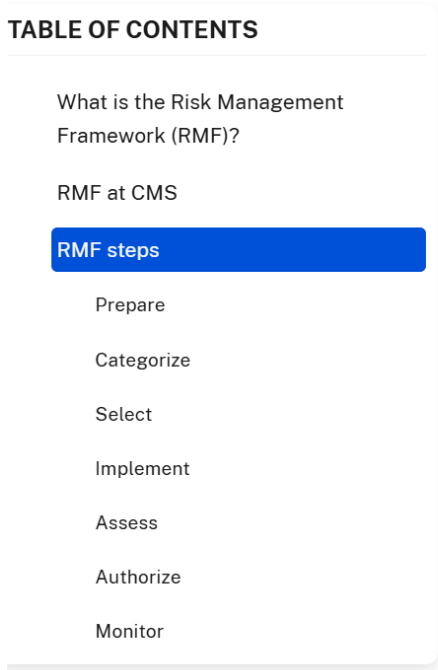
- ISPG worked with stakeholders to review the entire Governance, Risk and Compliance program (not just the GRC Tool, CFACTS).
- Over several months, each step of the Risk Management framework was examined to see what inputs, outputs and stakeholders were relevant to the CMS GRC Program.
- The CFACTS and Policy teams took the output of this initial collaboration developing a new CFACTS interface and redesigning RMF information on CyberGeek.
- The intention is to be able to use them side by side to complete the RMF steps required as part of the GRC program.

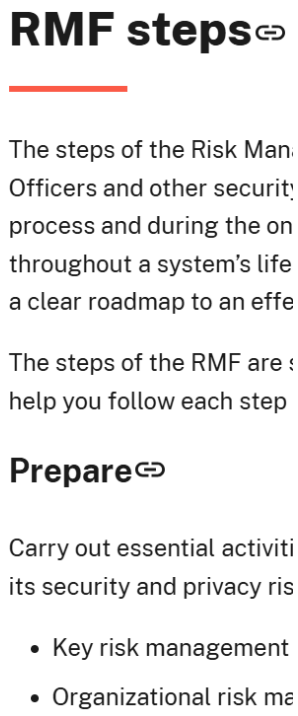
CFACTS User Interface Update



Tabs align with each Step of the RMF and correlate to the CyberGeek pages created for each of the steps.

As users open each tab in CFACTS, they can also open the corresponding page in CyberGeek to walk through each task required.





CyberGeek Risk Management Framework Pages

- Each task has a brief description of what the purpose of the task is.
- Potential inputs are listed and the purpose these inputs serve in the overall framework
- Expected outputs are detailed, showing what the expected result of completing the task properly
- Discussion section details what this task is trying to accomplish and what it means to CMS when this is completed properly.

Task S-6: Plan review and approval

Task S-6 involves reviewing and approving the security and privacy plans for the system and its environment of operation. This ensures that the plans are complete, consistent, and satisfy the stated security and privacy requirements for the system.

Potential Inputs:

- The **security and privacy plans** for the system serve as the primary input for Task S-6. These plans outline the selected controls and their intended application to meet security and privacy requirements.
- The **organization- and system-level risk assessment results** provide context for reviewing the security and privacy plans. They help ensure that the selected controls effectively mitigate identified risks and vulnerabilities.

Expected Outputs:

The primary output of Task S-6 is the approval of the security and privacy plans by the authorizing official or designated representative. This approval signifies that the plans are acceptable and can proceed to the next phase of the RMF process.

Discussion:

CyberGeek and CFACTS Demos

- Demo of CyberGeek And CFACTS

Questions