Infrastructure Operations Cybersecurity Management (ICSM) OVERVIEW

Timothy Amerson

Director and Cybersecurity Product Line Manager

Infrastructure Operations (IO)

Development, Security, and Operations (DevSecOps)

Office of Information and Technology (OIT)

October 2021

VA | U.S. Department of Veterans Affairs
Office of Information and Technology
Development, Security, and Operations

Department of Veterans Affairs Cybersecurity Drivers

Laws and Regulations, Government Policy, Guidance, and Best Practices

Executive Order 14028: Improving the Nation's Cybersecurity

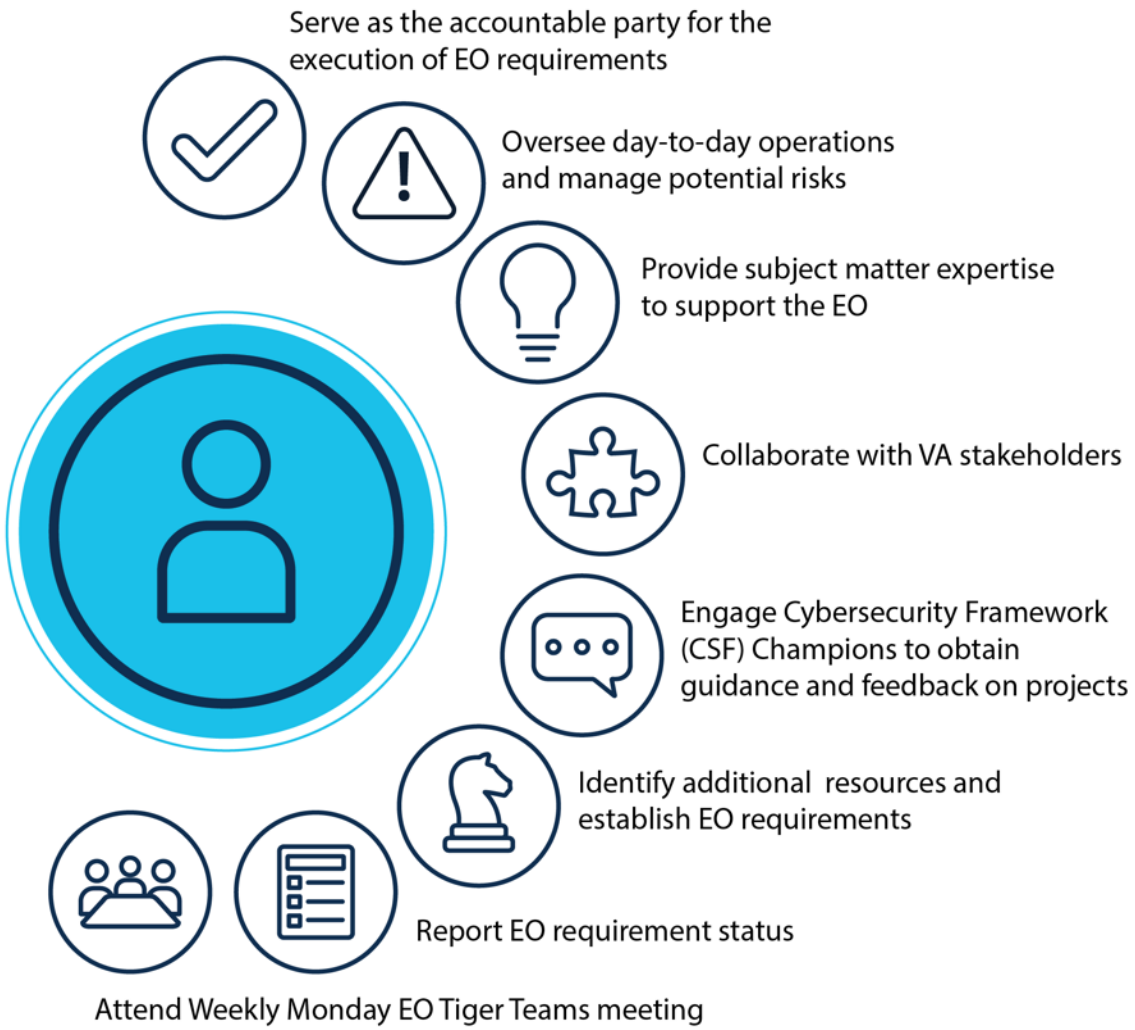
VA EO Tiger Team SES and Supporting VA POC Alignment

- Task: Cloud Adoption
  - Action: Adapt existing plans to use cloud technology.
- Task: Zero Trust Architecture
  - Action: Develop a plan for proactive security.
- Task: Multifactor Authentication (MFA) and Data Encryption
  - Action: Report on VA's progress in adopting MFA and encrypting data at (due every 60 days until adoption by agency).
- Task: Continuous Diagnostics and Mitigation (CDM)
  - Action: Establish and continually update CDM program.
- Task: Software Supply Chain Security
  - Action: Apply practices of least privilege, network segment, and configure security measures for critical software.
- Task: Unclassified Data
  - Action: Evaluate and report on sensitivity of unclassified data.
- Task: Investigative and Remediation Capabilities and Data Logging
  - Action: Demonstrate compliance with requirements on logging and retaining data.
- Task: Endpoint Detection and Response (EDR)
  - Action: Deploy initiative to support incident detection and response.
- Task: Incident Response Playbook
  - Action: Demonstrate compliance with DHS and CISA playbook on incident response plan.
- Task: Updates to the Federal Acquisition Regulation (FAR)
- Action: Update cybersecurity requirements (dependent on FAR Council review updates, expected no sooner than 120 days from May 12, 2021)

For more information on the EO, please visit the EO 14028 Team Site.

Executive Order Tiger Team Responsibiities

Responsibilities as an Executive Order (EO) Tiger Team Member



Responsibilities of the EO Tiger Team Leads (Associate Deputy Assistant Secretary – DevSecOps and Deputy CISO)

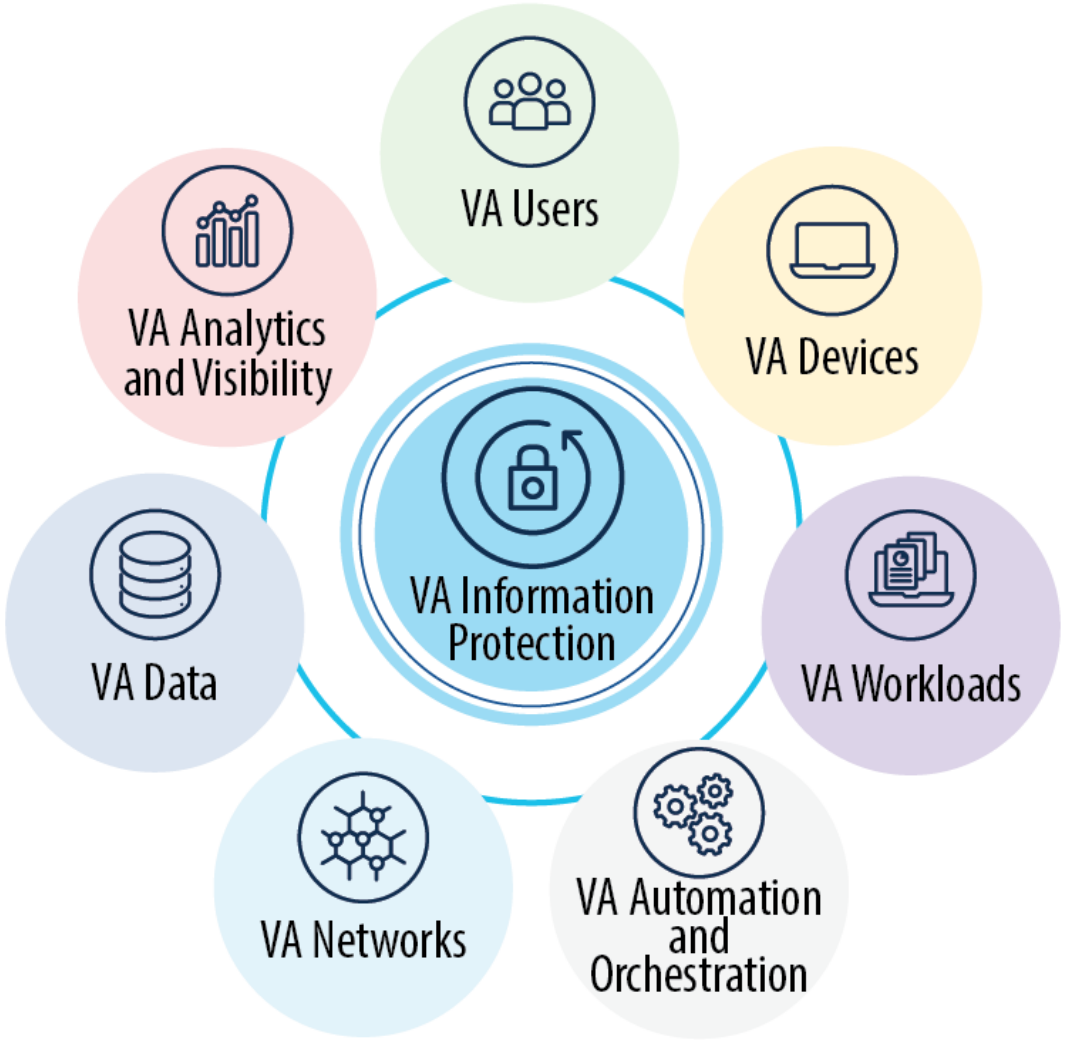
Executive Order 14028 and Zero Trust Architecture

Executive Order (EO) 14028 focuses on Improving the Nation's Cybersecurity

This EO requires VA to modernize its cybersecurity and move towards a Zero Trust Architecture. Within 60 days of this EO's date, VA needs to:

- **Develop a plan to implement Zero Trust Architecture**, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, **describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them**;
- Provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plans required pursuant to the plan to implement Zero Trust Architecture.

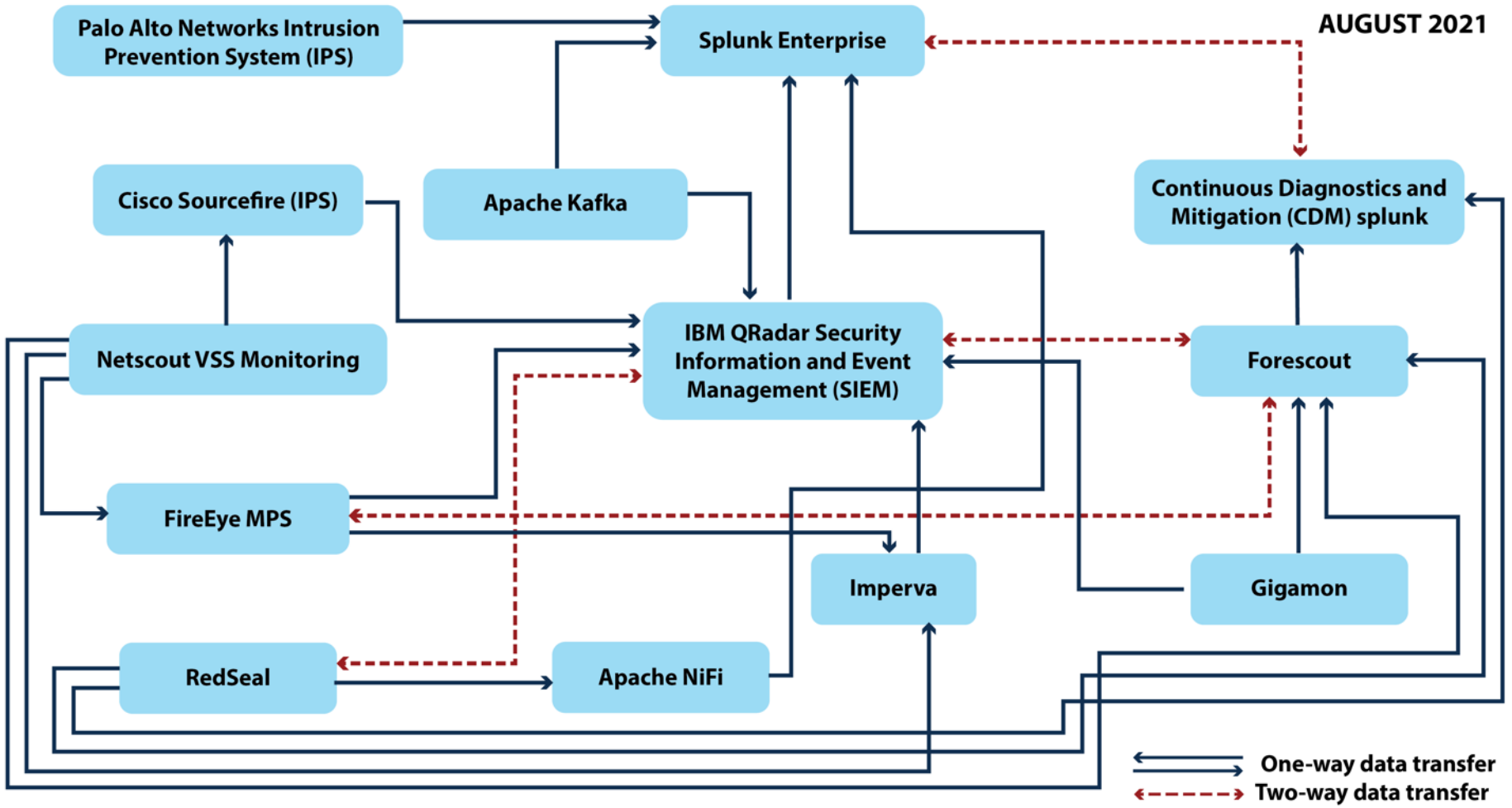
Zero Trust Basics



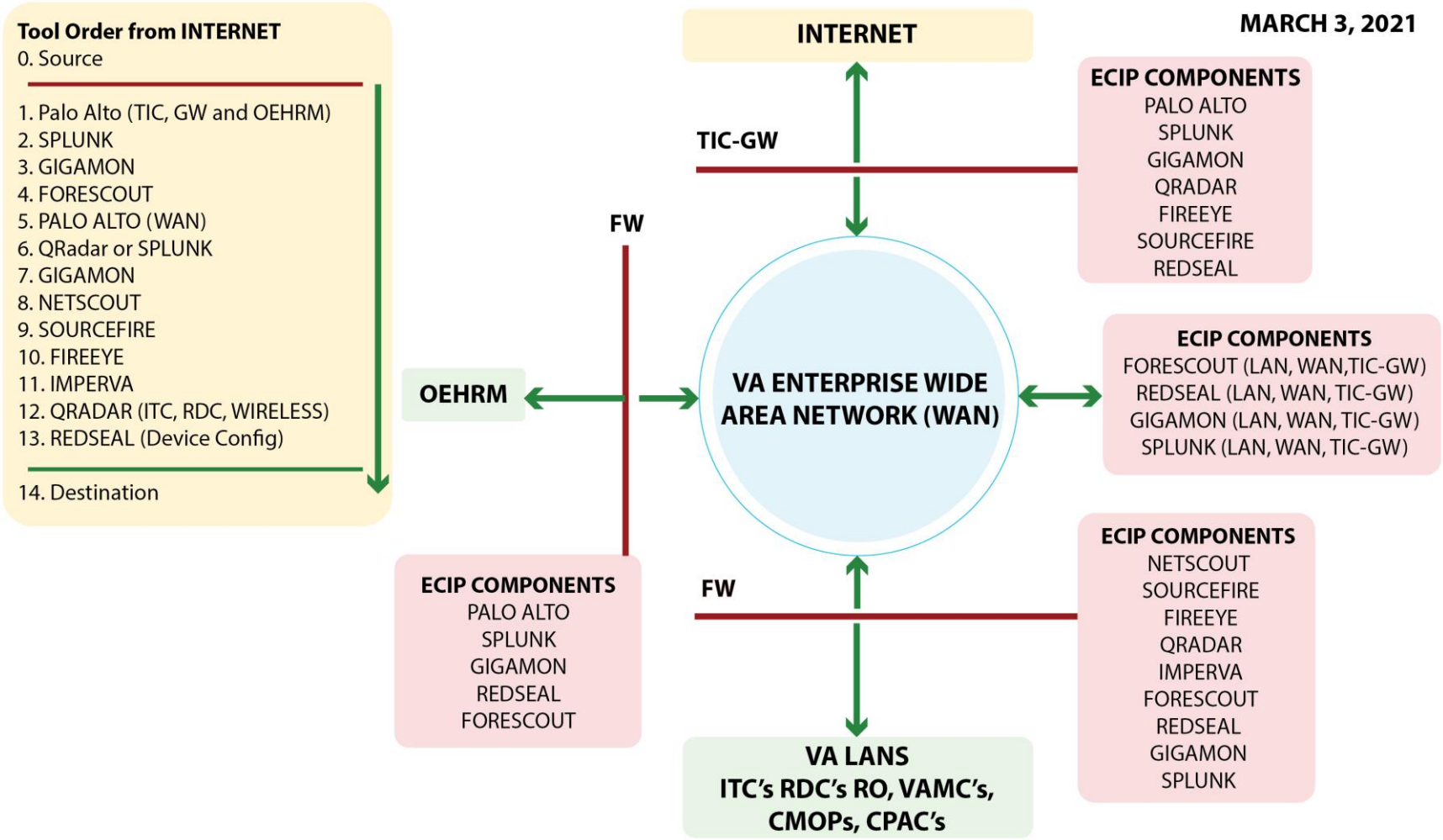
Principles:

1. Never trust, always verify
2. Assume breaches; eliminate the concept of trusted networks
3. Every device, user, application, and data flow is authenticated and authorized. All access to data and assets must be approved by dynamic policies
4. Use multiple data sources to establish confidence levels for access to resources

Enterprise Cybersecurity Infrastructure Protection (ECIP)



Enterprise Cybersecurity Infrastructure Protection (ECIP) Tool Visibility



DevSecOps Priorities

Priority 8 – Security Integration

Value Statement

Secure technology is an essential enabler to VA's mission. It serves as a fulcrum in providing greater access and improving the quality of our services.

We must be diligent in maintaining robust and resilient technology platforms through a unified, risk-based, operational approach.

With the Veteran in mind, we must recognize both the capabilities and risks associated with the tools we use and information they access.

DevSecOps Security Integration Priority – Highlights

1. **SECURITY FIRST**
   - Security is a key component within all of our activities and efforts; it cannot be an afterthought.
2. **PROVIDE EXCELLENT CUSTOMER SERVICE**
   - Deliver high quality products and services at velocity; do not compromise our security.
3. **EVOLVE BOUNDARIES**
   - Continue to mature our systems as we build, deliver, and operate products and services.
4. **ADOPT DEVSECOPS**
   - Adopting the DevSecOps framework results in secure system, customers, employees, and Veterans.

DevSecOps Security Integration Priority – Values

Secure technology is an essential enabler of VA's mission—to provide greater access and improve the quality of our services.

- **We must be diligent** in maintaining robust and resilient technology platforms through a unified, risk-based, operational approach.
- **We must be mindful** of both the capabilities and risks associated with the tools we use and information they access; always keeping Veterans in mind.

DevSecOps Security Integration Priority – Initiatives

1. Match DSO implementation strategy with VA's cybersecurity strategy
2. Streamline and expand communications
3. Establish and execute security governance
4. Establish and execute a budget that reflects DSO security lines
5. Secure and protect VA and Veteran Information
6. Secure and protect VA IT infrastructure and systems

Security Technology Roadmap

QUESTIONS?