Incident Management

Homeland Security

Verdis Spearman
verdis.spearman@hq.dhs.gov
703.235.5443

Agenda

- Overview
- Governance
- Stakeholders
- Responsibilities
- Trusted Internet Connection Initiative
- Incident Response Requirements

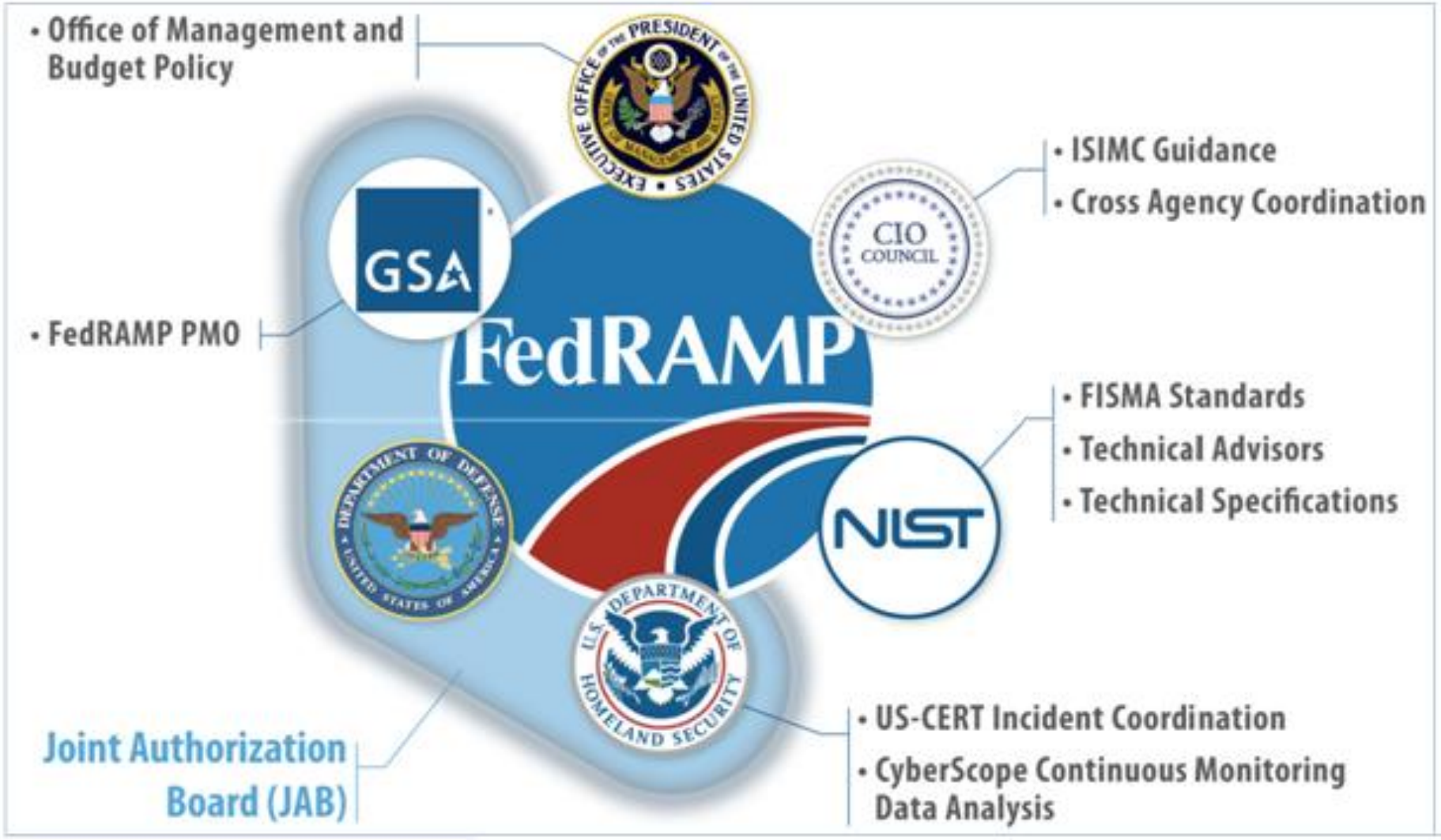
Overview

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

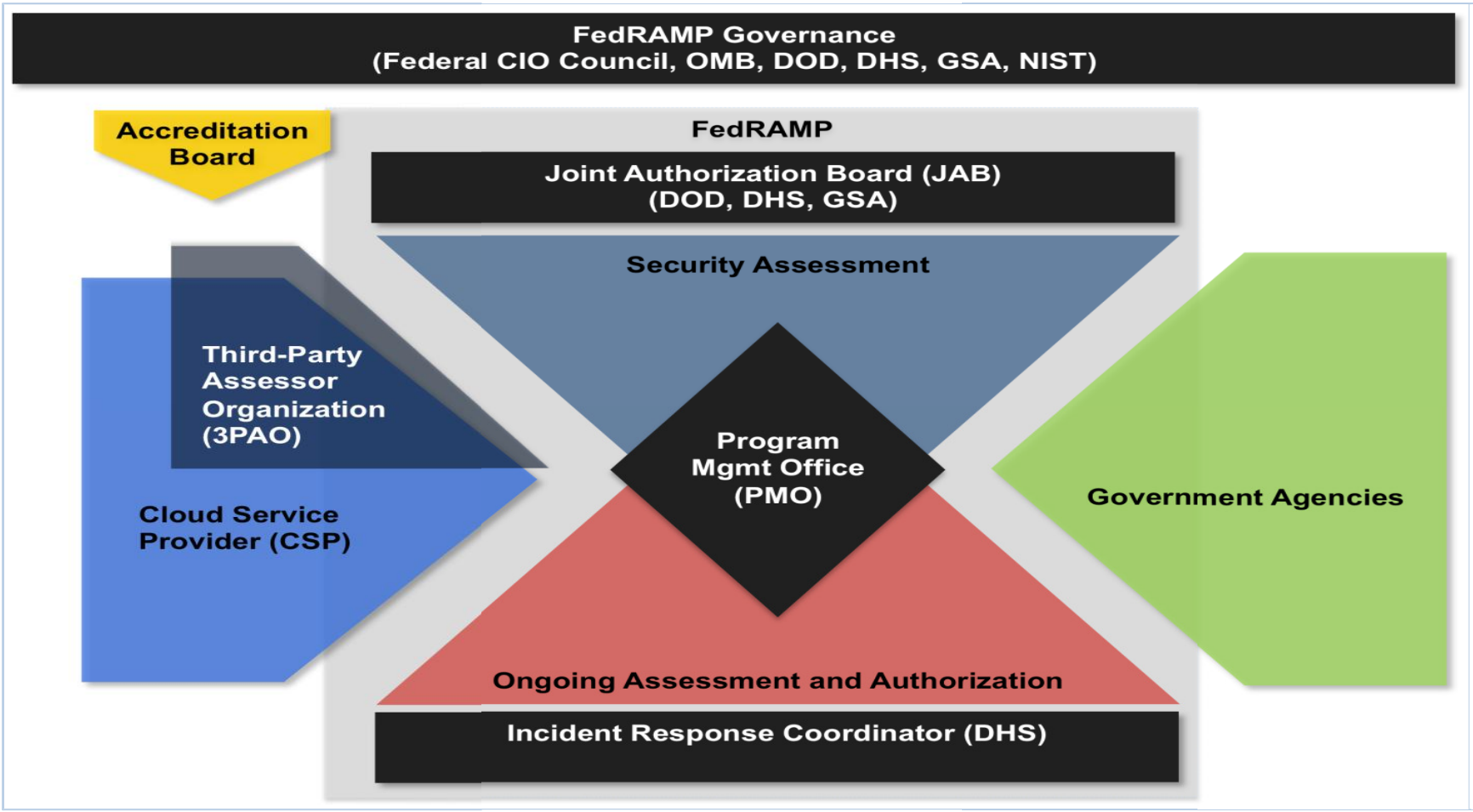
- Ensures that cloud based services have adequate information security;
- Eliminates duplication of effort and reduce risk management costs;
- Enables rapid and cost-effective procurement of information systems/services for Federal agencies.

Source: FedRAMP CONOPs, Version 1.0, 12 February 2012

Governance


• Office of Management and Budget Policy
• ISIMC Guidance
• Cross Agency Coordination
GSA
CIO COUNCIL
• FedRAMP PMO
FedRAMP
• FISMA Standards
• Technical Advisors
• Technical Specifications
NIST
Joint Authorization Board (JAB)
• US-CERT Incident Coordination
• CyberScope Continuous Monitoring Data Analysis

Stakeholders



Responsibilities

Department of Homeland Security

- Assist government-wide and agency-specific efforts to provide adequate, risk- based and cost-effective cyber security
- Coordinate cyber security operations and incident response
- Develop continuous monitoring standards for ongoing cyber security of Federal Information systems
- Monitors and reports on security incidents and provides data feeds for continuous monitoring.
- Develop guidance on agency implementation of the Trusted Internet Connection (TIC) program with cloud services

Federal Departments and Agencies

- Assess, authorize and continuously monitor security controls that are the Agency's responsibility
- Provide a POC for CSPs to communicate with
- Notify US-CERT when a CSP reports an incident
- Work with CSPs to resolve incidents by providing coordination with US-CERT
- Notify CSPs if the Agency becomes aware of an incident that a CSP has not yet reported
- Monitor security controls that are agency responsibilities
- Notify ISSOs if a CSP has reported an incident.

Cloud Service Provider Either commercial or agency operator

- Implement security controls based upon FedRAMP security baseline
- Create security assessment packages in accordance with FedRAMP requirements.
- Maintain Continuous Monitoring programs
- Comply with Federal Requirements for Change Control and Incident Reporting

Source: FedRAMP CONOPs, Version 1.0, 12 February 2012

Trusted Internet Connection Initiative

- FedRAMP Security Control SC-7(1) references the Trusted Internet Connection (TIC) initiative.

- The TIC initiative is mandated by OMB in Memo M-08-052. The purpose of putting in place Trusted Internet Connections (TIC) is to reduce and consolidate and connections to the federal government, including connections to the Internet.

- Data must pass through the TIC to obtain monitoring services from US-CERT.

Source: Guide to Understanding FedRAMP , Version 1.0, June 5

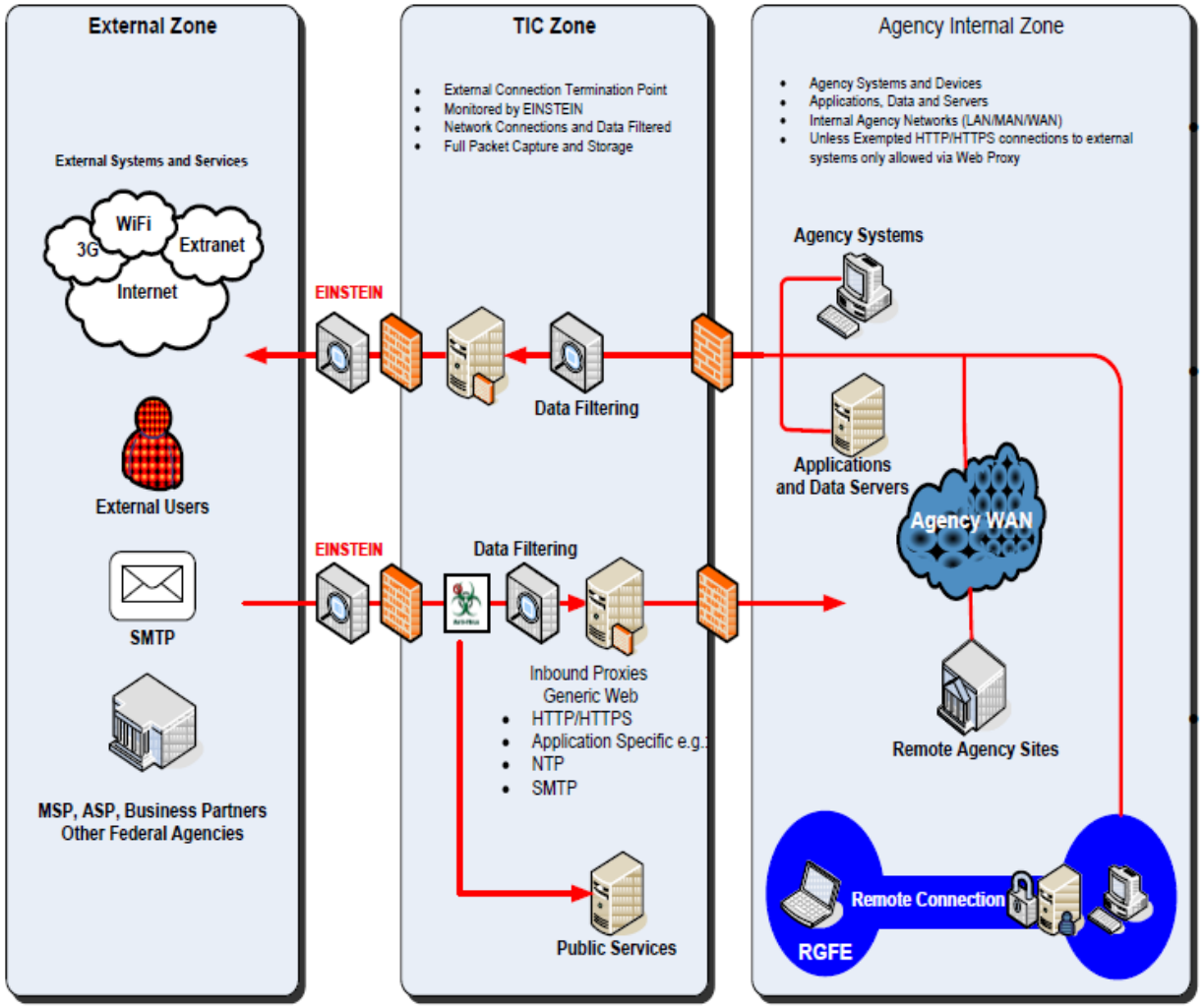
Currently, there are two categories of TICs:

- Federal agencies that are approved TIC Access Providers (TICAPs)

- Networx Managed Trusted IP Service providers with qualified and approved capabilities (MTIPS).

Source: Guide to Understanding FedRAMP , Version 1.0, June 5

TIC Core Concept



External Zone

- Outside Agency C&A Boundary
- Agency has no direct control over the security controls
- Public Internet and Business Partner networks

TIC Zone

- Border between internal and external resources
- Access point for external connections
- Traffic is monitored by National Cyber Protection System (NCPS), operationally known as EINSTEIN

Internal Zone

- Inside Agency C&A Boundary → Agency WAN
- Agency has direct control over its security policy and controls

Security Control SC-7 (1)

For a commercial cloud service provider to comply with SC(7)-1, the CSP must demonstrate an architecture that allows an agency to provide effective separation of network traffic to meet the following objectives:

1. CSP routes all Government traffic via VPN back to an agency network.

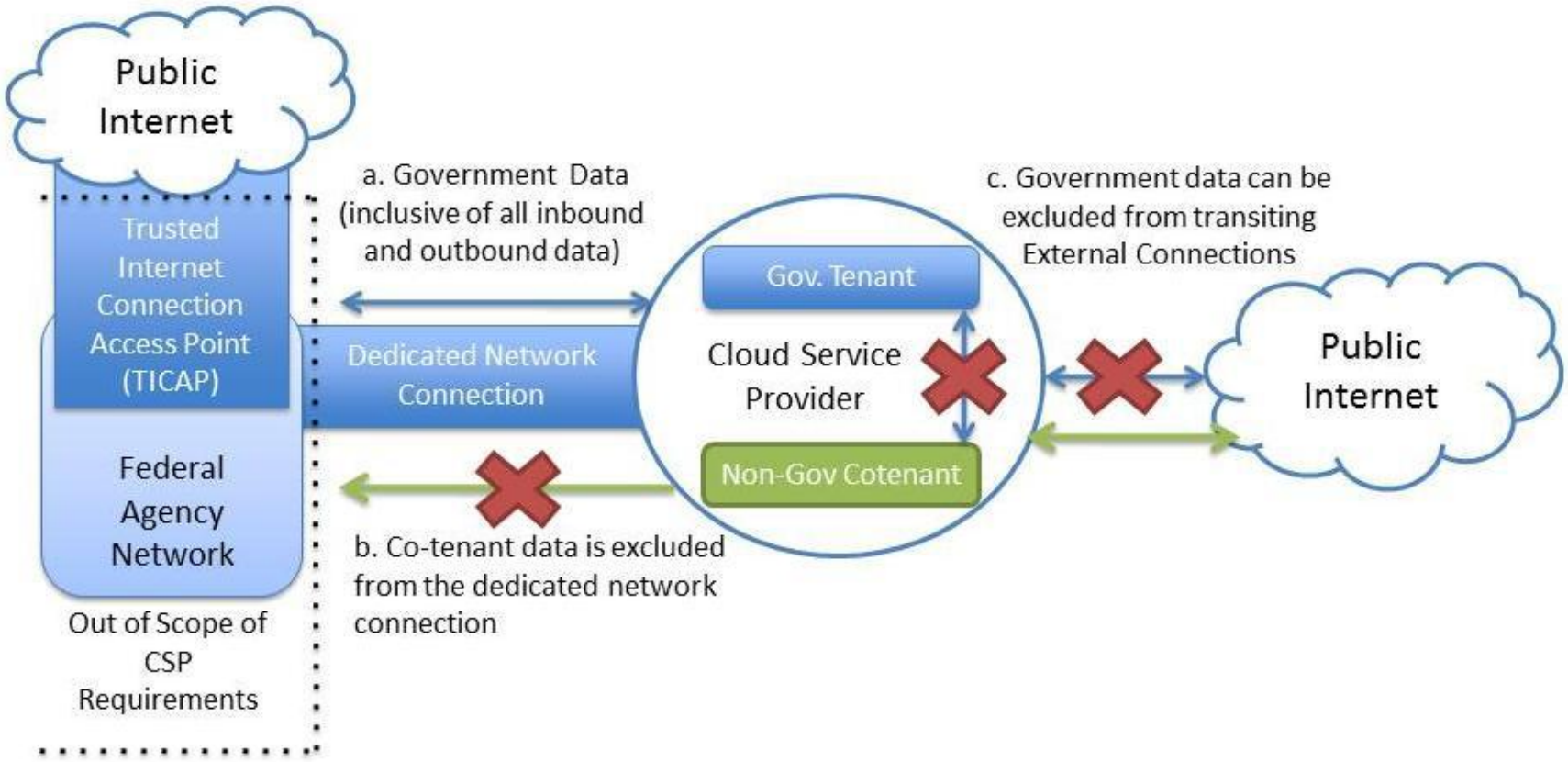
2. CSP routes all government traffic through an agency sponsored TICAP or MTIPS, no government traffic is allowed over the public Internet.

3. CSP routes all government traffic through dedicated network connections to an agency network, no government traffic is allowed over the public Internet.

4. CSP routes by all government traffic through government endpoints, not allowing any data to traverse any other end-points than agency IP address ranges (effectively all inbound/outbound traffic routes through government network by proxy or other rules).

Source: Guide to Understanding FedRAMP , Version 1.0, June 5

TIC Boundary



Source: Guide to Understanding FedRAMP , Version 1.0, June 5

Incident Response Plan

The System Security Plan requires a description of the CSP's incident handling capability. The Incident Response Plan should stand alone.

- How do you prepare for incidents?
- Who should agency customers call if they suspect an incident?
- Is there an incident hotline or phone number published where customers can see it?
- What capability do you have to detect incidents?
- If you suspect an incident how do you verify if it really is an incident?
- What methods do you use to analyze confirmed incidents?
- What methods do you use to contain incidents?

Source: Guide to understanding FedRAMP, Version 1.0, June 5, 2012

Incident Response (IR) Controls

FedRAMP requires that CSPs develop an Incident Response Plan that describes how they manage security incidents for the system and address the Incident Response (IR) family of security controls below:

- IR-1 Incident Response Policy and Procedures
- IR-2 Incident Response Training
- IR-3 Incident Response Testing & Exercises
- **IR-4 Incident Handling**
- IR-5 Incident Monitoring
- **IR-6 Incident Reporting**
- IR-7 Incident Response Assistance
- IR-8 Incident Response Plan

Source: Guide to Understanding FedRAMP , Version 1.0, June 5

Incident Handling

Security Control IR-4 requires CSPs to employ incident handling techniques and processes. CSP incident handling capabilities required by this control should be documented in the Incident Response Plan.

- CSP shall report an incident to an affected agency,

- The agency will escalate incidents to US-CERT according to the agency's own respective Incident Response Plan instructions.

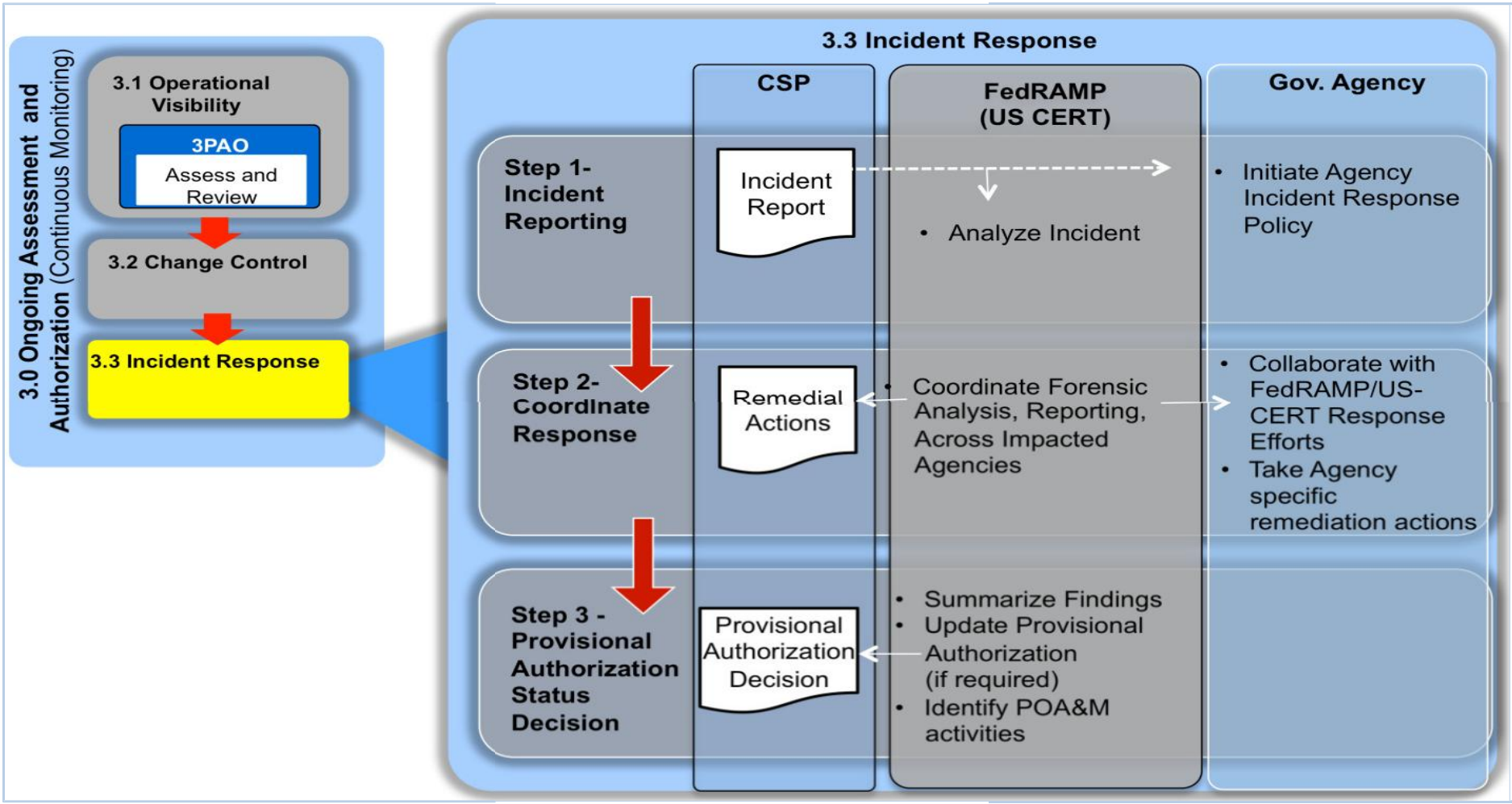
- The agency should forward to US-CERT the Incident Reporting Form that was filled out by the CSP.

- If an agency discovers an incident that has not been reported to them by the CSP, the agency should contact the CSP using the incident contact information provided in the CSP's Incident Response Plan.

- Agencies should offer to coordinate assistance between US-CERT and CSPs when CSPs report incidents to agencies.

- Though CSPs should be fully capable to handle incidents, in coordination with their customer agencies, CSPs may also obtain additional assistance from US-CERT.

Notional Incident Response Process



Methods of Reporting incidents to US-CERT

Online

https://forms.us-cert.gov/report/

Email

soc@us-cert.gov

Phone

(888) 282-0870


US-CERT - United States Computer Emergency Readiness Team - Windows Internet Explorer
http://www.us-cert.gov/
Live Search
File Edit View Favorites Tools Help
Convert Select
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
SECURITY PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
ABOUT US
GFIRST
United States Computer Emergency Readiness Team
US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans. US-CERT's vision is to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a complex environment.
Learn more about US-CERT »
Home and Business
Government
Control Systems
I Want To
Report an incident
Report a software vulnerability
Report phishing
Subscribe to Alerts
Receive security alerts, tips, and other updates.
Enter your email address
Sign Up
Mailing Lists and Feeds
Contact Us
(888) 282-0870
Send us email
Download PGP/GPG keys
Home | FAQ | Contact Us | Traffic Light Protocol | Privacy & Use | Get a PDF Reader
US-CERT is part of the Department of Homeland Security.
Internet
75%

Value of Reporting

- Establishes a history of activity
- Empowers subscribing Agency's security authorities and analysts to react and trigger appropriate control mechanisms
- Cross government trend analysis
- Enhances Federal Enterprise Wide Situation Awareness

FedRAMP Documents

http://www.gsa.gov/portal/category/102991

Homeland Security

Verdis Spearman
verdis.spearman@hq.dhs.gov
703.235.5443