


Security Event and Incident Handling Procedure for CFPB

This process addresses DOJ's Security Event and Incident Handling between the Justice Security Operations Center (JSOC) and the Consumer Finance Protection Bureau (CFPB). The key stakeholders in this process are JSOC, and CFPB stakeholders.

Scope

This process includes non-emergency and emergency security events and incidents, and support provided during working hours and after working hours.

Event Definitions

Event	Description
Non-Emergency (Standard) Security Event	Events that are identified via active monitoring or input from non-JSOC teams and do not pose any immediate threat to the CFPB environment
Emergency Security Event	<div>Outages, Distributed Denial of Service (DDoS) with a confirmed impact, malware outbreaks, or other significant events that impact the CFPB's Mission Essential Functions (MEFs).</div> <div><ul style="list-style-type: none">Require immediate government interventionDeemed urgent by the designated CFPB POC </div> <div>Note: During normal business hours, degradations of service would also require notification of (POCs)</div>

Intake: Identify and Triage Events

The purpose of this phase of the process is to characterize the event and determine whether the event is a security incident.

- Non-emergency events
 - Identified by JSOC
 - Identified by CFPB, reported to JSOC
- Emergency events
 - Identified by JSOC
 - Identified by CFPB, reported to JSOC

The JSOC utilizes playbooks, continually updated, with specific actions to be taken, based on the attack vector/type of potential incident. The JSOC refers to the communication plan developed by DOJ and CFPB during onboarding to include the appropriate CFPB POCs.

The following chart provides an overview of the JSOC and CFPB stakeholders involved in the reporting of events and potential security incidents.

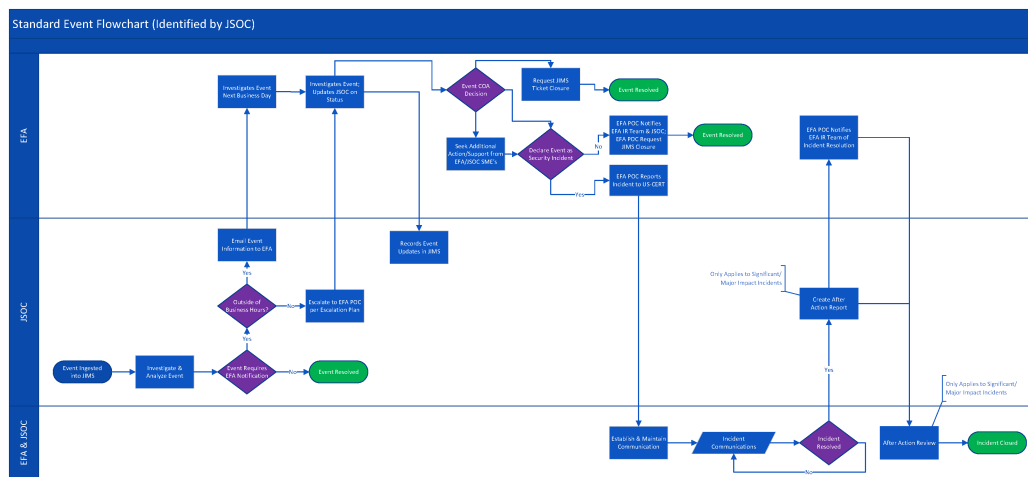
Stakeholder	Non-Emergency Events detected by JSOC	Emergency Event, detected by JSOC	Non-emergency Events, reported by CFPB to JSOC*	Emergency Event, reported by CFPB to JSOC*
JSOC Watch Floor	Triages event and creates incident ticket, if applicable	Reports to CFPB in accordance with (IAW) communication plan	Triages email or call from CFPB and creates incident ticket	Triages email or call from CFPB and creates incident ticket
CFPB CISO	Receives report of potential incident via email from JSOC	Contacted by JSOC IAW communication plan	Receives report of potential incident via email from JSOC and/or by CFPB Service Desk	Contacted IAW communication plan
CFPB Security Team or Computer Security Incident Response Team (CSIRT)	Copied	Contacted by JSOC IAW communication plan	Reports to JSOC an event identified through an escalated internal IT issue	Contacted IAW communication plan
CFPB Technical Team (e.g., desktop, platform, cloud, O365, etc.)	N/A	Contacted by JSOC IAW communication plan	N/A	Contacted IAW communication plan Reports to JSOC
CFPB Service Desk, if applicable	N/A	Contacted by JSOC IAW communication plan	Reports to JSOC an event identified through an end-user report, for example	Reports to JSOC

***Note:** Non-emergency and Emergency events reported by the CFPB to JSOC are not sourced by JSOC detections and accessible CFPB log sources. Events in the category could be identified through reports of end-user issues and escalated to CFPB Technical Teams, identified by the CFPB security team, CFPB's independent assessor, or 3rd party vendors.

If Event is a [Non-Emergency](#), identified by JSOC

Step #	Incident Response Actions
1	Event is automatically ingested by Jira from the CFPB log data sources via DOJ SIEM, and shows up in the Justice Incident management System (JIMS) triage channel.
2	JSOC, within specified timeframe, will review the event, perform analysis, and determine if the event should be reported to the CFPB as a potential incident.
3	If escalation is required, JSOC contacts CFPB IR Mailbox via email with information about the event in the body of the email.
4	CFPB CSIRT investigates the event. If outside of normal business hours, CFPB CSIRT addresses it the next business day.
5	CFPB CSIRT addresses the event (either clarification or remediation) and responds to JSOC via email, including JIMS ticket number in email subject line.
6	JSOC records event information in JIMS (automatic ingest of all emails with the JIMS ticket number).
7	CFPB's CSIRT team member assigned to the incident has three courses of action they can take: <ul style="list-style-type: none"> a. Review and request closure of the JIMS ticket (and related security events) b. Seek additional action from CFPB CSIRT members, CFPB CISO, or JSOC c. Declare the event as a security incident. Report the incident to US-CERT per CFPB policies.
8	If the event is not declared an incident, CFPB POC notifies CFPB CSIRT Team and JSOC via email and requests closure in JIMS.

Note: For major and significant incidents, JSOC involves CFPB CSIRT in its after-action review and provides results to CFPB POCs for review. See below for definition of major or significant incidents.

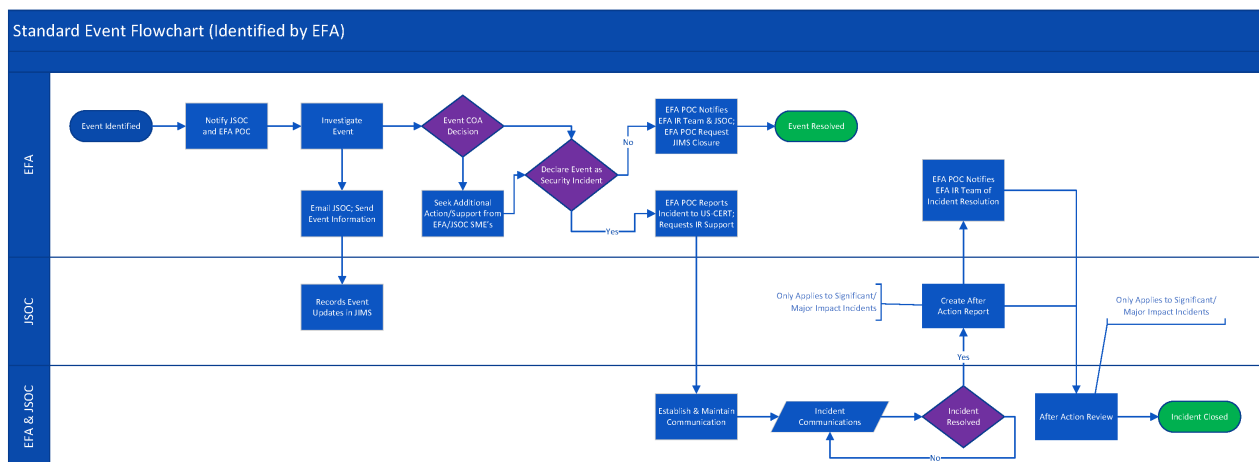


If Event is a [Non-Emergency](#) Identified by CFPB

Step #	Incident Response Actions
1	CFPB CSIRT sends email to JSOC and cc's CFPB CISO. <ul style="list-style-type: none"> a. Note: This step is applicable 24x7.
2	CFPB CSIRT investigates the event using the existing process outlined in CFPB's IRP, collecting as much information as possible prior to contacting JSOC, as appropriate for business hours.
3	CFPB CSIRT addresses the event and informs JSOC via email, the type of incident and its assessed criticality/severity.
4	CFPB CSIRT team member assigned to the incident has two courses of action they can take: <ul style="list-style-type: none"> a. Seek additional action from CFPB CSIRT members, CFPB CISO, or JSOC b. Declare the event as a security incident. Report the incident to US-CERT per CFPB policies.

5	If the event is not declared an incident, CFPB POC notifies CFPB CSIRT Team and JSOC via email and requests closure in JIMS.
6	If the event is declared an incident, CFPB POC notifies CFPB CSIRT Team and JSOC via email and requests JSOC incident response assistance.

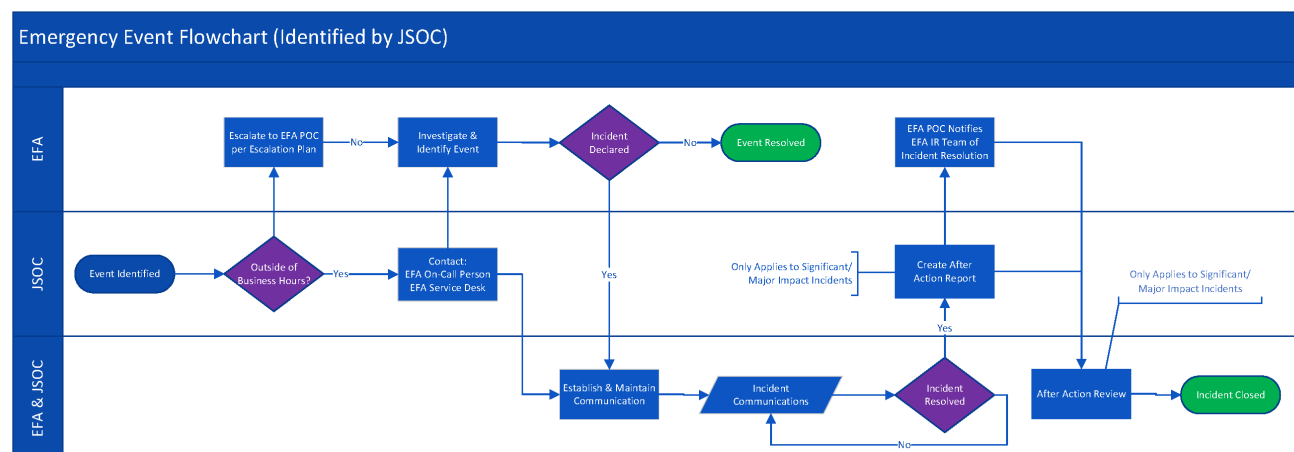
Note: An example of a CFPB Identified Non-Emergency event could be CFPB CSIRT team members witnessing a large data upload to Amazon AWS where appropriate approvals have not been granted.



If Event is an **Emergency** Identified by **JSOC**

Step #	Incident Response Actions
1	JSOC immediately escalates to CFPB CSIRT, and notifies the CFPB distribution list a. Note: If outside of normal business hours, JSOC will use the On-Call phone list to contact the CFPB CSIRT member and CFPB technical team POCs on call.
2	When and if CFPB formally identifies an event as an incident, JSOC and CFPB set up and maintain communications (including use of CFPB IR Mailbox) and command and control as appropriate throughout management of the security incident.
3	Input into the incident history (i.e., Containment, Eradication, and Recovery activities) requires that the CFPB IR Mailbox and JSOC IR mailbox be used by all involved parties for all incident updates. For situations where email is not a viable means of communication, CFPB and JSOC will use a pre-determined out-of-band communications.
4	Once the incident is resolved and is ready to be closed, CFPB CISO notifies CFPB CSIRT Team and JSOC via email and requests closure in JIMS.

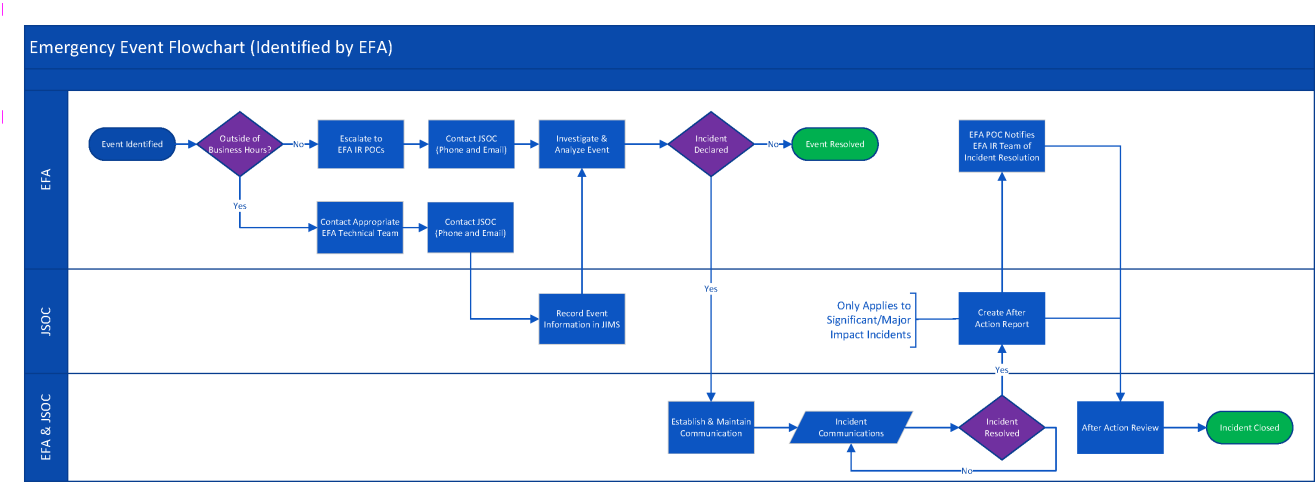
Note: For major and significant incidents, JSOC involves CFPB CSIRT in its after-action review and provides results to CFPB CISO for review.



If event is an Emergency Identified by CFPB

Step #	Incident Response Actions
1	CFPB CSIRT immediately escalates to CFPB POCs (per CFPB IRP) and contacts JSOC via phone and email. a. Note: If outside of normal business hours, CFPB Service Desk or CFPB CSIRT contacts the appropriate CFPB technical teams and JSOC via phone and email.
2	When and if CFPB formally identifies an event as an incident, JSOC and CFPB set up and maintain communications (including use of CFPB IR Mailbox) and command and control as appropriate throughout management of the security incident.
3	Input into the incident history (i.e., Containment, Eradication, and Recovery activities) requires that the CFPB IR Mailbox and JSOC IR mailbox be used by all involved parties for all incident updates. For situations where email is not a viable means of communication, CFPB and JSOC will use a pre-determined out-of-band communications.
4	Once the incident is resolved and is ready to be closed, CFPB CISO notifies CFPB CSIRT Team and JSOC via email and requests closure in JIMS.

Note: An example of a CFPB-identified Emergency event would be CFPB IT Ops noticing unusual activity on the DNS servers, leading to the identification of a DDoS attack.



Definition of Major and Significant Incidents

Major Incident

Any incident that is likely to result in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.^[1]

Breach that constitutes a Major Incident

A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

Significant Cyber Incident

A Significant Cyber Incident as defined by PPD-41, United States Cyber Incident Coordination is a cyber incident that is (or a group of related cyber incidents that together are) likely to result in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.