InCommon Federation Security Incident Handling Framework

Prepared by: Nicholas Roy, Director of Technology and Strategy, InCommon
Version: 1.2
Date: February 27, 2017

Document Title: InCommon Security Incident Handling Framework
Repository ID: TI.100.1
DOI: 10.26869/TI.100.1
Persistent URL: http://doi.org/10.26869/TI.100.1
Authors: Nick Roy
Publication Date: January 30, 2017
Sponsor: InCommon Steering Committee
Superseded documents: None
Proposed future review date: March 1, 2019
Subject tags: federation, trust, incommon

Change Log

Status	Change	Date	Version	Approved by
Draft	First version to InCommon Steering	October 21, 2016	0.6	Nicholas Roy
Draft	Added example of “upstream provider” in Scope section	October 26, 2016	0.7	Nicholas Roy
Draft	Added information about vulnerability disclosure to scope and contact sections, acknowledged TIER Security and Audit Working Group input	November 2, 2016	0.8	Nicholas Roy
Draft	Added contact information	January 11, 2017	0.9	Nicholas Roy
Prepublication	Added governing language reference	January 19, 2017	1.0	Nicholas Roy
Publication	Revisions from Internet2 General Counsel	January 30, 2017	1.1	Nicholas Roy
Publication	Revisions to fix typos and add document repository information	February 27, 2018	1.2	Nicholas Roy

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Governing Language

The InCommon Federation Operating Policies and Practices [1] document states, as of July, 2016:

10.3.1 - Suspension for reasons of security

> *A Participant may request the suspension of any Federation services in the case of Administrator credential compromise, participant key compromise, or other security compromise within the Participant's systems. This request may be made via e-mail or telephone from the Executive or Administrator and will be verified by InCommon using trusted communication channels. Suspension may include processes such as revoking credentials, or removing or modifying Metadata.*
>
> *If InCommon suspects any compromise or negligence on the part of a Participant, it will make reasonable efforts to contact Participant to resolve the issue. In the case of a significant security incident that poses an unacceptable risk to InCommon or other federation participants, InCommon may take immediate remediation actions commensurate with the impact of the incident.*

Mission Statement of InCommon CSIRT

InCommon's Computer Security Incident Response Team (CSIRT) is a group of identified individuals working at Internet2 and in the community, assigned specific roles, and chartered to respond to security incidents related to InCommon's trust, identity and security-related services so that they may be relied upon by InCommon participants for mission-critical and security-sensitive operations on an ongoing basis. To that end, the InCommon CSIRT will:

- Receive information about security-related threats to InCommon infrastructure
- Receive information about security-related threats to InCommon participants' federating systems
- Assess the risk of such threats
- Develop response and remediation plans where appropriate to address these threats
- Execute, with the possible addition of needed external resources, incident response according to a documented incident handling framework
- Report out to stakeholder communities on the nature of incidents responded to, status of response, and to communicate as needed with affected parties

Definition of "Security Incident"

A computer security Incident is: A violation or imminent threat of violation of computer security policies, applicable laws and regulations, acceptable use policies, or standard security practices. A security incident may involve either electronic or paper data. [5]

Initial Contact/Notification and Triage

Any party may make InCommon's CSIRT aware of a relevant security incident or disclosure via one of the following mechanisms (available 24x7x365)

1) ***Call this number: +1 734 352 7045 (PREFERRED)***
2) ***Send an email to: security@incommon.org***

NOTE: Outside of normal US business hours, it may take up to 12 hours for staff to be notified of your email. In critical emergencies, please call the phone number above, if possible.

Inquiries from any law enforcement agency regarding a security incident, including formal legal process such as subpoenas and warrants, must be directed to the General Counsel of Internet2.

DO NOT communicate any sensitive information via these channels. InCommon Federation staff will set up a secure communications channel with you, if need be, after your initial request is received

InCommon's CSIRT will accept, evaluate and reply (when necessary and deemed appropriate) to valid submissions as soon as possible, but in no event later than 24 hours after receipt of the notice.

Generalized Procedure for When Action Is Required

Upon receipt of information about a possible security threat to InCommon, the CSIRT will:

1. Identify an incident handling lead
2. Assign the lead to perform a brief initial assessment of the situation, including initial classification of the incident or disclosure as: "Normal," "Escalation," or "Emergency" in nature.
3. The lead will determine and execute next steps based on assessment of initial event classification, including the formation of an incident handling team as necessitated by nature, criticality and scope. Lead may call in resources for the incident handling team, and those resources are obligated to help with further analysis, remediation and other necessary incident handling steps. Normal procedures to follow are documented in the Incident Handling Actions Matrix below
4. All relevant details of the incident including classification, handling, communication, resolution and disposal will be documented at the request of Counsel in a shared file repository within Internet2
5. An incident is closed when the Executive Sponsor determines that the event has been handled appropriately and is no longer an active threat. In some cases, one or more reports may be issued to relevant stakeholders.

Roles

Roles 1-4 make up the standing CSIRT, with all roles under 5 filled on an as-needed basis.

1. CSIRT Executive Sponsor, typically the Internet2 Vice President for Trust and Identity Services
2. Incident Lead, typically an InCommon technical director or manager
3. Incident Communications Representative, typically an Internet2 marketing and communication director
4. REN-ISAC liaison
5. Incident Handling Team (***specific make-up of each team subject to availability and appropriateness*** at the discretion of the Incident Lead and CSIRT Executive Sponsor)
    a. Lead (a role which may be assigned to any of the team members, but should remain lead throughout the handling of an incident)
    b. Executive Sponsor

c. Steering Liaison
d. Ops Advisory Liaison
e. InCommon Operations Representative
f. Internet2 Communications Representative
g. Internet2 Chief Information Security Officer Representative
h. Other relevant internal Internet2 areas
i. REN-ISAC Representative and Liaison
j. Law enforcement Representative and Liaison
k. Legal Representative

Assessment of an Incident

This section is a set of guidelines to allow the named incident handling lead to assess the classification of an incident, for use as input in determining next steps, in the next section.

Scope

To be in scope for action by InCommon's CSIRT, mitigation of the incident must essentially depend on one or more changes to InCommon's operations which involve InCommon's change management processes, as determined by the CSIRT.

An incident or disclosure which has compromised, or may lead to the compromise of, systems or services that affect one or more of:

1) InCommon Operations or its upstream or third-party providers (for example, cloud hosting providers, multifactor authentication providers, etc.) on which its operations depend.
2) The systems or services of an InCommon Participant relevant to federation participation, such as Identity Provider or Service Provider software or related cryptographic materials.
3) Any other operational aspect of InCommon's trust services.

are deemed to be in-scope for InCommon's incident handling processes and should be assessed for nature and criticality before any further actions are taken. If an incident is not in-scope, it will be documented and handed off to the appropriate party (internal to or external to InCommon) for further assessment and handling.

Nature

Answer the question: Is the event an "Incident"? i.e.:

1. Discovery of the neglect of a system or systems by a human actor responsible for maintaining that/those systems that prevents misuse or exploitation of the system(s) to

harm InCommon or its participants' networks or systems as those networks or systems function in a core or supporting role within the portfolio of Incommon trust services.
2. Use of a system or network in any way that compromises InCommon or its participants' networks or systems as those networks or systems function in a core or supporting role within the portfolio of InCommon trust services.
3. Any other use or misuse of computing resources, intentional or otherwise, which would cause harm to networks or systems that have a core or supporting role within the portfolio of InCommon trust services (for more information on InCommon services, see: https://www.incommon.org/).
4. Disclosure of a security vulnerability known to affect systems or services used in the operation of InCommon's infrastructure.

If an event is determined to be an "Incident" in nature, it should be further analyzed for elements of criticality in order to determine necessary actions. If the event is not an "Incident," it should be handed off to InCommon Operations for further analysis and handling.

Criticality

Incidents fall into three criticality categories:

Normal - an event that does not affect critical production systems or the trustworthy flow of identity/trust-related data across InCommon services.

Escalation - an event that affects production systems and requires change control steps be followed as part of a response.

Emergency - a change to a production system impacting one or more of the following:

1) Health and safety
2) Critical controls on systems which are relied upon for the trustworthy exchange of identity/trust data between InCommon participants and which utilize InCommon services for facilitation of this data exchange
3) Ability of InCommon or one or more of its participants to provide services or conduct business via InCommon services
4) Anything deemed an emergency by virtue of related InCommon policies or the CSIRT Executive Sponsor

Events that are "Escalation" or "Emergency" in nature should be acted upon by the Incident Lead in coordination with the incident handling team according to the Incident Handling Actions Matrix in the next section. Events that are "Normal" will be handed off to the relevant party for further handling.

Communications

Communication of an incident is a critical step in the response plan, to be formulated in accordance with the matrix below. It is important that a communication plan be designed in a way that does not disclose information about an incident to an inappropriate audience. In many cases it is also important to let InCommon participants and other stakeholders know about an incident in a timely manner based on their need to know and need to share indicators of compromise. At a minimum, for an Escalation or Emergency-level Incident, an after-action review will be prepared at the request of Counsel. The review will include root cause analysis and remediation steps, and should be conducted by the Incident Lead, and a report should be prepared which may be shared with appropriate audiences.

A designated communication representative should be named as part of each Escalation or Emergency-level incident. This person will provide needed input to a decisionmaking process about what information to share with which audiences, and in particular, what information may be shared outside of Internet2 and the CSIRT, when, via what channels, and in what format. The Executive Sponsor will have ultimate authority for decisionmaking about the release of information, in consultation with the Incident Lead.

Traffic Light Protocol for Exchange of Information

For the purposes of communications with the CSIRT and with external parties during the handling of an active incident (and for further information sharing with other parties after the incident), the Traffic Light Protocol [3] must be used as a way to identify, label, and ensure compliance with scoping of the information shared. The Incident Lead, Executive Sponsor and Communications Representative are primarily responsible for assigning TLP categories to information to be shared, although there are times when other members of the CSIRT and external parties will need to make an assessment about TLP categories and label information they are sharing. When there is uncertainty on the part of a party responsible for classification on the proper classification of a communication item, the party should verify with the CSIRT or incident handling team. Generally, the originator of new information will need to appropriately initially label that information.

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Reference: TLP levels matrix, from US-CERT [4]

Incident Handling Actions Matrix

This matrix is intended as a generalized guide for the broad steps required in the classification and handling of security-related events. The matrix below is partially derived from information available from EDUCAUSE [2]

All information known by InCommon relating to the security incident, including, as applicable, log files and other digital evidence, will be retained by InCommon for 7 years.

	Normal	Escalation	Emergency
Gather incident facts and prepare Initial Assessment of Situation and send to CSIRT	X	X	X
Contact the Legal representative and begin preparing all material at the request of Counsel	X	X	X
Determine whether Protected Identity Information or Protected Health Information is involved	X	X	X
Legal Representative determine whether to notify insurance carrier	X	X	X
Contact Executive Sponsor		X	X
Convene CSIRT Members on established realtime communication channel		X	X
Deliver initial assessment to CSIRT team via secure channel	X	X	X
Re-Assess Nature, Scope and Criticality in conference		X	X

	If re-assessment leads to a demotion to “Normal” criticality, document and delegate further handling to non-CSIRT team(s). If re-assessment supports original or higher assessed criticality execute further steps in the table.	If re-assessment supports original or higher assessed criticality execute further steps in the table.	If re-assessment supports original assessed criticality execute further steps in the table.
Lead determine whether external help is required, if so, request Exec to engage appropriate help		X	X
Lead determine initial remediation steps, distribute to CSIRT team via secure channel		X	X
Executive determine whether or not to involve other needed representatives or resources		X	X
CSIRT team conference and agree on remediation steps, timeline, dependencies, and *initial* notification requirements. These decisions are documented by the Lead or designee.		X	X
CSIRT team engage relevant actors using		X	X

Traffic Light Protocol, to act on remediation plan, ensuring discretion on the part of needed actors			
CSIRT and action team act on plan		X	X
CSIRT team evaluate post-action situation and develop initial report to Executive		X	X
Executive conferences with CSIRT team and determines need for further measures, next steps, and reporting requirements, including complying with all applicable laws and regulations. These decisions are documented by the Lead or designee.		X	X
CSIRT team and executive act on any needed next steps and reporting requirements		X	X
CSIRT team conducts an after-action review as part of security continuous improvement process. These decisions are documented by the Lead or designee.		X	X

Appendix A: Foundational Documents

[1] InCommon Federation Operating Policies and Practices

[2] West Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, Zajicek. Handbook for Computer Security Incident Response Teams (CSIRTs) April, 2003. Carnegie-Mellon University Software Engineering Institute, CMU/SEI-2003-HB-002

[3] EDUCAUSE, Sensitive Data Exposure Checklist v1.1

[4] US-CERT, Traffic Light Protocol

[5] NIST SP800-61, Computer Security Incident Handling Guide

Appendix B: Acknowledgements

Thanks to the following individuals and groups for their contributions to this document:

Kim Milford, REN-ISAC
Thomas Barton, The University of Chicago
Jane Drews, The University of Iowa
InCommon Technical Advisory Committee
InCommon Steering Committee
REN-ISAC
Big Ten Academic Alliance CISOs
EDUCAUSE
Internet2 and InCommon Staff
Internet2 General Counsel
Internet2 TIER Security and Audit Working Group