



This document is scheduled to be published in the Federal Register on 06/28/2013 and available online at <http://federalregister.gov/a/2013-15542>, and on FDsys.gov

Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number: 130417383-3383-01]

Computer Security Incident Coordination (CSIC): Providing Timely Cyber Incident Response

AGENCY: National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION: Notice; Request for Information (RFI)

SUMMARY: The National Institute of Standards and Technology (NIST) is seeking information relating to Computer Security Incident Coordination (CSIC). NIST is seeking this information as part of the research needed to write a NIST Special Publication (SP) to help Computer Security Incident Response Teams (CSIRTs) to coordinate effectively when responding to computer security incidents. The NIST SP will identify technical standards, methodologies, procedures, and processes that facilitate prompt and effective response.

This RFI requests information regarding technical best practices, current practices, impediments to information sharing and response, risks of collaborative incident response, the role of technology and standards in incident coordination, specific technical standards and technologies that have been found helpful (or ineffective), opportunities for improvement, viewpoints on incident coordination objectives, and suggestions for guidance. In developing the SP, NIST will consult with the Department of Homeland Security, the National Security Agency, other interested federal agencies, the Office of Management and Budget, and individually with other parties who respond to this RFI to discuss their comments and seek further information. The SP will be developed through an open public review and comment process that may include workshops as needed.

DATES: Comments must be received by 5:00 PM Eastern time on [PLEASE INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]

ADDRESSES: Written comments may be submitted by mail to Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899. Submissions may be in any of the following formats: HTML, ASCII, Word, RTF, or PDF. Online submissions in electronic form may be sent to incidentcoordination@nist.gov. Please submit comments only and include your name, company name (if any), and cite “Computer Security Incident Coordination” in all correspondence. All comments received by the deadline will be posted at <http://csrc.nist.gov> without change or redaction, so commenters should not include

information they do not wish to be posted (e.g., personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: For questions about this RFI, contact:

Lee Badger, National Institute of Standards and Technology, 100 Bureau Drive,
Gaithersburg, MD 20899-8930, telephone (301) 975-3176, e-mail lee.badger@nist.gov.

Please direct media inquiries to NIST's Office of Public Affairs at (301) 975-NIST.

SUPPLEMENTARY INFORMATION:

The nation is increasingly reliant on secure and reliable operation of computing systems throughout Federal Government, key industrial sectors, and civil society. Unfortunately, modern computing systems frequently are exposed to various forms of cyber attack. In some cases, attacks can be thwarted through the use of defensive technologies, such as anti-virus scanning, cryptographically-protected communications, access control, or authentication mechanisms. Despite careful use of defensive technologies, however, some systems will be successfully attacked. When a successful attack occurs, the job of a Computer Security Incident Response Team (CSIRT) is to detect that an attack occurred, prevent ongoing damage, repair the damage to the extent possible, reconstitute the affected system functions, and report as appropriate to the United States Computer Emergency Readiness Team (US-CERT) and to other affected parties according to governing regulation and law. Maintaining a security response capability is a complex and challenging undertaking, and in order to assist those in charge of security efforts,

NIST has published guidance, such as NIST SP 800-61 Revision 2 “Computer Security Incident Handling Guide.”¹

NIST SP 800-61 provides guidance on how to establish and operate an incident response capability. The guide provides information on developing procedures for performing incident handling and reporting, for structuring a team, staffing, and training. The guide defines an incident response life cycle encompassing four phases: preparation, detection and analysis, containment eradication and recovery, and post-incident activity. Although the NIST incident handling guide focuses primarily on how to handle incidents within a single organization, it also provides high-level guidance on how a CSIRT may interact with outside parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. This guidance focuses primarily on understanding team-to-team relationships, sharing agreements, and the role that automation techniques may play in the coordination of incident response.

This RFI seeks information for a substantial expansion of NIST guidance in how multiple CSIRTs may work together to coordinate their handling of computer security incidents and how CSIRTs might work together with other organizations within a broader information sharing community. This information will serve as input to a new NIST SP, 800-150, “Computer Security Incident Coordination.” The goal of this planned document is to provide guidance for cross-organizational incident response, particularly focusing on improving the overall response during cross-cutting and widespread incidents,

¹ <http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf>

inspiring effective information sharing practices, and fostering interoperability between teams with varying capabilities. The new SP 800-150 will supplement the existing NIST incident handling guide, SP 800-61, by significantly expanding the guidance on coordination and information sharing (section 4 of SP 800-61). Although work on SP 800-150 may produce guidance that eventually contributes to a revision of SP 800-61, the focus of SP 800-150 will be on the coordination aspects of incident response.

For the purposes of this RFI, the term “incident coordination” is defined as communication and collaboration with external entities during an incident response such that:

- Two or more organizations are involved.
- There is an exchange of information between organizations pertaining to incidents or indicators of incidents.
- The organizations work together to achieve common goals (i.e., fast, effective incident response).
- The organizations limit exposures of sensitive information.

NIST seeks information regarding technical best practices, current practices, impediments to information sharing and response, risks of collaborative incident response, the role of technology and standards in incident coordination, specific technical standards and technologies that have been found helpful (or ineffective), opportunities for improvement, viewpoints on incident coordination objectives, and suggestions for guidance.

Request for Information

The following questions cover the major areas about which NIST seeks information. The questions are not intended to limit the topics that may be addressed. Responses may include any topic believed to have implications for effective incident coordination regardless of whether the topic is included in this document.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received by the deadline will be made available publically at <http://csrc.nist.gov/>.

General Incident Coordination Considerations

1. What does your organization see as the greatest challenge in information sharing throughout the incident response lifecycle?
2. Describe your organization's policies and procedures governing information sharing throughout the incident lifecycle. Also describe to what degree senior management is involved in defining these policies and procedures.
3. What role does senior management have in the execution of your policies and procedures?

4. To what extent is information sharing incorporated into your organization's overarching policies and processes?
5. How much of your incident handling effort is spent on the different phases of the incident handling lifecycle (from NIST SP 800-61): (1) preparation, (2) detection-and-analysis, (3) containment-eradication-and-recovery, (4) post-incident-activity.
6. What are the relevant international, sector-specific or de facto standards used or referenced by your organization to support incident handling and related information sharing activities?
7. How do you determine that an incident is in progress (or has happened)?
8. How do you determine that an incident has been handled and requires no further action?
9. How do you determine when to coordinate and/or share information with other organizations regarding an incident?
10. Do you have documented case studies or lessons learned to share (good or bad examples)? If so, please provide URLs or attachments with your response.

Organizational Capabilities and Considerations for Effective Incident Coordination

Incident handling teams and coordinating centers often collaborate at varying stages of the incident management lifecycle described by NIST SP 800-61. Within this context, individual organizations may offer specific capabilities and may have specific considerations related to effective incident coordination.

1. Do you maintain a list of key contacts for use during an incident? If so, are these contacts identified as individual people, or as positions?
2. What is the size of your organization (e.g. staff, contractors, members)? How many individuals are involved in incident coordination activities carried out by your organization?
3. Relative to the incident response lifecycle defined by NIST SP 800-61, what aspects of incident coordination occur within your organization?
4. What services and assistance (e.g. monitoring, analysis, information) does your organization provide to others both inside and outside your organization relating to incident coordination?
5. Does your organization have any method for understanding and describing the quality or sensitivity of different types of information shared by a third party? For each type of information, can you describe the method?

6. Approximately how many employees (please indicate full time or part time as appropriate) do you devote to incident response?
7. If possible, list examples of highly effective computer security incident response teams and comment on what made them successful.
8. Based on your personal or your organization's experience, what are the most and least effective communication mechanisms used (e.g., phone, email, etc.) when coordinating an incident, and why? In what order do you typically use specific communication mechanisms?
9. Do you have examples of alternate communication mechanisms used because an incident has degraded communications?
10. Do you hold regular incident review meetings? Between organizations? How frequently? If your team does not hold incident review meetings regularly, why not?
11. What skillsets (e.g., network sniffing, system administration, firewall configuration, reverse engineering, etc.) does your organization need most when an incident is in progress?
12. Are there incident handling and response skillsets that are specific to your industry or sector?

13. How do those skills relate to information sharing and communication before, during and after an incident?

Coordinated Handling of an Incident

1. Do you report incidents or indicators to US-CERT?
2. Do you coordinate incident response with organizations other than US-CERT?
3. Do you participate in an incident coordination community such as the Defense Industrial Base (DIB), the Defense Security Information Exchange (DSIE), or an Information Sharing and Analysis Center (ISAC)? What are the benefits? Are there any pain points?
4. How is information about threats and/or incidents shared among coordination community members?
5. How do you prioritize incidents?
6. How do regulatory requirements affect your organization's ability or willingness to share information or collaborate during an incident?

7. What regulatory bodies are you required to report information to regarding incidents? For each regulatory body, what kind of information does your organization report and what has been your organization's reporting experience?

Data Handling Considerations

1. What, if any, types of information would create risk or disadvantage if shared by your organization?
2. What kinds of information would you never share with a peer during incident handling?
3. What types of protections, redactions, or restrictions would aid your organization in sharing information?
4. Do you use specialized formats to communicate incident information?
5. What do you see as the pros and cons of specialized formats for representing and communicating incident information?
6. What incentives exist for your organization to share information with other organizations during an incident?

7. What disincentives exist that might prevent your organization from sharing information with other organizations during an incident?

8. If available, please provide an example when sharing with other organizations proved to have negative implications for your organization's incident response.

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

Dated: June 24, 2013

Willie E. May
Associate Director for Laboratory Programs

[FR Doc. 2013-15542 Filed 06/27/2013 at 8:45 am; Publication Date: 06/28/2013]