Software Engineering Institute

Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0

John Haller
Samuel A. Merrell
Matthew J. Butkovic
Bradford J. Willke

April 2011

TECHNICAL REPORT
CMU/SEI-2011-TR-015
ESC-TR-2011-015

CERT Program

http://www.sei.cmu.edu

Carnegie Mellon

This report was prepared for the

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about SEI publications, please visit the library on the SEI website (www.sei.cmu.edu/library).

Table of Contents

Acknowledgments

The authors would like to thank the Department of Homeland Security, National Cyber Security Division; Jeffrey James Bryan Carpenter, Dr. Timothy Shimeall, Robin Ruefle, and Robert Floodeen of the CERT® Program for their feedback and insights on the operations of National CSIRTs; Peter McCarthy for his assistance in compiling the additional resources; and Amanda Parente and Lisa Gardner for their support in editing this document.

Executive Summary

Managing cyber security through a national strategy is necessary for all national governments in the 21st century. Critical infrastructure, from transportation and power generation to food supply and hospitals, depends on information and communications technology (ICT). Reliance on complex and constantly evolving technology is pervasive across all sectors of critical infrastructure. The complexity of these systems makes it difficult for national governments to understand and mitigate risks related to this technology.

Establishing and maintaining a computer security incident management capability helps nations manage this dependence. This capability is referred to in this document as a National Computer Security Incident Response Team (National CSIRT), but it can be implemented in a variety of different organizational forms. Beyond responding to discrete computer security incidents, a robust incident management capability enhances the ability of the national government to understand and respond to cyber threats. Operating a National CSIRT, or an organization like it, is a core component of a nation's overall strategy to secure and maintain technologies vital to national security and economic vitality.

This handbook is first in the *Best Practices for National Cyber Security* series. It is designed to be introductory curricula for capacity development within nations. The intended audience includes national leaders and managers who wish to learn more about the value of National CSIRTs and incident management capability generally. It is not intended to be a guide for the daily operation of a National CSIRT but as informative material on how National CSIRTs support a national cyber security strategy. It also outlines the first steps towards building this capacity.

The handbook provides principles and strategic goals to help nations develop their own, robust national management capacity. It attempts to alleviate the challenge of developing an incident management capability with limited published guidance. Many nations attempting to develop National CSIRTs have started by attempting to copy existing CSIRT organizations. This approach can be problematic because not every nation has the same needs and resources. The operating principles and strategic goals discussed in this document enhance the ability of governments to manage cyber security risks and focus their efforts.

Strategic goals are essential design requirements and imperatives. They serve as fundamental elements of an incident management capability and are meant to provide clarity and direction. This document proposes four strategic goals as they relate to a national computer security incident management capability.

1. Plan and establish a centralized computer security incident management capability (National CSIRT).
2. Establish shared situational awareness.
3. Manage cyber incidents.
4. Support the national cyber security strategy.

There is a common need to resist, reduce, and fight cyber threats and respond to attacks. National CSIRTs provide a domestically-focused, internationally-amplified operational response to cyber

incidents that destabilize global telecommunications, data services, supply chains, and critical infrastructure. We hope as a sponsor of a National CSIRT or similar capability, you will see these benefits and encourage your government and organizational leaders to participate in a global culture of security.

Abstract

As nations recognize that their critical infrastructures have integrated sophisticated information and communications technologies (ICT) to provide greater efficiency and reliability, they quickly realize the need to effectively manage risk arising from the use of these technologies. Establishing a national computer security incident management capability can be an important step in managing that risk. In this document, this capability is referred to as a National CSIRT, although the specific organizational form may vary among nations. Nations face various challenges when working to strengthen incident management, such as the lack of information providing guidance for establishing a national capability, determining how this capability can support national cyber security, and managing the national incident management capability. This document, first in the *Best Practices for National Cyber Security* series, provides information that interested organizations and governments can use to develop a national incident management capability. The document explains the need for national incident management and provides strategic goals, enabling goals, and additional resources pertaining to the establishment of National CSIRTs and organizations like them.

1 Introduction

Nations are increasingly dependent on complex systems and information technology. In many cases, information and communications technologies (ICT) vital to national and economic security are subject to disruption from a number of causes, either originating from within or outside the nation. Leaders in government and private industry are increasingly confronted with uncertainty about cyber risk and vulnerabilities. This uncertainty stems from the complexity and interconnectivity of evolving technology used to support critical systems. To ensure security and economic vitality, nations must manage cyber security in accordance with their own economic, social, and political considerations.

Implicit in a strategy for cyber security is establishing a national computer security incident management capability. Often this capability may take the form of one or more National Computer Security Incident Response Teams (National CSIRTs). Organizations such as the National CSIRT provide value in several ways. A National CSIRT coordinates incident management and facilitates an understanding of cyber security issues for the national community. A National CSIRT also provides the specific technical competence to respond to cyber incidents of national interest. In this primary role, the National CSIRT fills a planned response function, providing solutions to urgent cyber problems. The ability of National CSIRTs to identify cyber security problems and threats and disseminate this information helps industry and government secure current and future systems.

Beyond the capacity to react to specific incidents and disseminate information, National CSIRTs can assist government departments with aspects of their work that relate to information and communications technology. Law enforcement and the judiciary, for instance, are increasingly concerned by the movement of criminals to the virtual world to commit crimes ranging from child exploitation to financial fraud. The world's defense services rely on advanced information-technology based systems for their capabilities. And critical infrastructure relating to human security, such as food, water, and electricity supply chains depend on reliable technology.

National CSIRTs can also serve as a focal point for a national discussion on cyber security. Cyber security poses new and unique social, legal, and organizational challenges. The global interconnectedness of computer networks, the anonymity of online actors, and the rapid exploitation of vulnerabilities allow actions of individuals, often located outside national borders, to have serious and magnified effects on vital national systems. Meanwhile, governments are limited by the jurisdictional reach of their laws and the physical limits of their borders. The National CSIRT can promote a thoughtful discussion on these issues, engaging authorities in the fields of education, law, and governance, among others, to help create solutions that align with national character and traditions.

Finally, building a National CSIRT helps foster international cooperation on cyber security. A basic function for a National CSIRT is to act as the point of contact and facilitate communication about incidents with overseas requestors. Collaboration and cooperation with peer organizations can help analysts and leaders better understand global cyber threats and actors.

1.1 Intended Audience

The primary audience for this document consists of those sponsoring the development of a national computer security incident management capability, usually referred to as a National CSIRT. This document will discuss the considerations and goals inherent in standing up a National CSIRT. While the focus here is on a single National CSIRT organization, some nations may find it advantageous to house this capability across several organizations or agencies. The principles and recommendations in this document should be useful even to nations that do not choose to build a single National CSIRT organization.

1.2 About the *Best Practices for National Cyber Security* Handbook Series

The *Best Practices for National Cyber Security* series of handbooks is designed for leaders and key stakeholders in critical infrastructure protection, government, and industry, or anyone interested in cyber security policy and management. It is intended to be foundational material for individuals and organizations working to develop a strategy for national cyber security management. Each handbook in the series will provide a tailored message. In addition to this initial document, the series addresses topics such as:

- Using Critical Success Factors to Manage CSIRTs with National Responsibility[1]
- Public Private Partnerships in Cyber Security[2]
- Managing and Participating in Cyber Security Exercises
- Cyber Security Assessment and Evaluation

The subject matter presented in the other handbooks is formatted similarly but emphasizes unique functions of national cyber security in greater depth.

1.3 How to Read This Handbook

This document is structured to serve as a strategic education for building a computer security incident management capability. Because of the breadth of this topic, the focus here is on the creation of a National CSIRT. The material is intended to outline the stakeholders, constraints, and goals for National CSIRTs; to raise awareness of the need for this type of capability; and to frame this capability in the national strategy. While the focus is on National CSIRTs specifically, the guidelines herein are meant to help national leaders generally, regardless of the specific organizational form chosen to handle incident management.

The second section, *Setting the Context: National Cyber Security*, includes information about National CSIRTs as part of a larger national approach to cyber security. This section specifically discusses the importance of a national strategy, the context of a national cyber security policy framework, and an overview of key stakeholders in national cyber security as they relate to National CSIRTs. The special role of National CSIRTs is discussed.

Section 3, *Strategic Goals and Enabling Goals for Incident Management Capability*, introduces a hierarchy of goals for ensuring alignment between the National CSIRT and national cyber securi-

[1] To be published in May 2011

[2] To be published in May 2011

ty strategy. The *Strategic Goals* subsections outline long-term imperatives while the *Enabling Goals* subsections highlight the necessary steps to build an operational National CSIRT capacity.

Section 4 offers a case study of national incident management in the United States. It includes an explanation of how the U.S. Department of Homeland Security (DHS) operates the National Cyber Security and Communications Integration Center. The handbook is concluded in Section 5.

2 Setting the Context: National Cyber Security

Not all risk is owned and mitigated by a nation's government. The national and local government and its various branches, critical infrastructure owners and operators, and citizens share this responsibility. New and emerging risks must be effectively identified, analyzed, and mitigated to ensure the safety and security of daily life for citizens. These risk management activities may involve ensuring continuity of government, safeguarding electricity generation, overseeing emergency response services, or securing a reliable supply chain, among others. Each of these activities relies heavily on information technology in a modern economy. National leaders realize that the security of information and information technology is a priority and should be codified in laws and national strategy. Chief among the strategies for enhancing this security are specific operational capabilities, such as the incident management activities typically performed by a National CSIRT.

2.1 The Importance of a National Strategy for Cyber Security

Building a national strategy for cyber security is the first step in establishing a national cyber security program. A national policy framework should explain the importance of cyber security, help stakeholders understand their role, and set goals and priorities. The national strategy should integrate security fundamentals (such as raising awareness) and emphasize cooperative relationships among national stakeholders. The national strategy can also serve as a backdrop for the creation of laws that relate to areas such as computer crime, the protection of intellectual property, and privacy.

The goals that a nation identifies and promotes through its strategy align the program to a consistent vision and establish a clear direction for the efforts of the program. The strategy should include sufficient detail to allow stakeholders—including the National CSIRT—to understand the stated goals and evaluate their progress toward achieving them. Finally, the national strategy should reconcile the need for security with the rights of citizens, as well as national values and norms.

The National CSIRT should be deliberately aligned with national cyber security strategic goals to ensure that its work contributes to achieving them. While establishing a national strategy is the first step, doing so may not always be feasible. Getting a large number of stakeholders to agree on a strategy can be difficult. Alternatively, national leaders may judge that the need to establish an incident management capability is more pressing than creating a fully integrated strategy. In these cases, creating an effective strategy may occur concomitantly with building incident management capability. Regardless, the National CSIRT sponsor or proponent should work with the government to consider national needs and priorities throughout the process of building a National CSIRT.

2.2 Key Stakeholders of National Cyber Security

Cyber security has many stakeholders. This section broadly describes the roles and responsibilities of typical national stakeholders and how they might contribute to a national cyber security program. These roles are not unique to National CSIRT operations, but many of the stakeholders

discussed here may directly interact with the National CSIRT. Moreover, the National CSIRT can enhance its role and help advance a security culture by proactively interacting with these stakeholders.

Governments have a multitude of roles and responsibilities to strengthen national cyber security. Their primary role is to define the national strategy and provide the policy framework. The policy framework describes the architecture by which the national efforts are built and operated. Following that, the government has a responsibility to participate with all stakeholders in efforts to identify, analyze, and mitigate risk. The government also has a key role to play in the arena of international relations and cyber security, particularly in the creation of treaties relating to cyber security and the harmonization of national laws relating to cybercrime.

2.2.1 Executive Branch of the Government

In most nations, the executive branch enforces laws and ensures security. It also may include the military. The executive branch is often the sponsor of the national cyber security program and must ensure that the cyber security program remains viable and has appropriate resources (for example, is authorized, staffed, funded, and so on).

2.2.2 Legislative Branch of the Government

The legislative branch provides effective laws that promote cyber security. Whether through appropriations of resources or funding, legislation that mandates execution of the national strategy, privacy or tort laws, or laws that establish criminal behaviors, the legislature must ensure that the national cyber security program has the necessary support.

2.2.3 The Judiciary

The nation's judiciary and legal institutions provide clarity and consistency in areas of law that can affect cyber security. Privacy law is an example of one of these areas. By working with their global counterparts, the legal community can limit the ability of criminals and other malicious actors to take advantage of differences in legal jurisdictions.

2.2.4 Law Enforcement

Law enforcement ensures that legislation related to cyber security is enforced. Additionally, law enforcement can serve as an important source of intelligence about malicious activity, exploited vulnerabilities, and methods of attack. Sharing this information allows critical infrastructure owners and operators to learn from others' experiences and improve security practices and management. Law enforcement can also enhance cyber security by cooperating with counterparts in other nations on the pursuit and apprehension of international criminal actors.

2.2.5 Intelligence Community

The intelligence community plays an important watch and warning role for technical infrastructure. Intelligence organizations usually monitor various sources for threats and vulnerabilities to a nation's infrastructure. This information should be distilled and provided to the National CSIRT and, where appropriate, to infrastructure owners. This distribution of information helps both groups efficiently anticipate, recognize, and resolve attacks.

2.2.6 Critical Infrastructure Owners and Operators

Critical infrastructure components depend on the nation's economic system and technological sophistication, among other factors. A general definition for critical infrastructure is

> *Systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*[3]

Critical infrastructure owners and operators are important stakeholders in the nation's overall cyber security strategy. Infrastructure operators typically understand how security threats and vulnerabilities affect their sector. This knowledge frequently includes proprietary systems and software, such as Supervisory Control and Data Acquisition Systems (SCADA). Infrastructure operators also implement security recommendations or mandates created by the national government and other authorities. They must reconcile the need for security with the occasionally contradictory goals of efficiency and profitability.

Because of their unique position, infrastructure owners and operators frequently possess valuable information, ranging from the actual software problems and cyber attacks they might experience, to the efficacy of countermeasures or risk mitigation strategies. They are also a primary consumer of information about security vulnerabilities. Because of their practical experience implementing security standards and complying with the law, owners and operators may have valuable input into the development of effective, realistic rulemaking and legislation.

2.2.7 Vendors

Vendors of information technologies and services contribute to national cyber security through development practices and ongoing vulnerability reduction efforts. Vendors are often the source of vulnerability information; they ensure that users have up-to-date information and technical solutions to mitigate known vulnerabilities. Ideally, vendors will cooperate with National CSIRTs and extend the analytical and problem-solving capabilities the National CSIRT needs to conduct incident response. Information sharing among vendors, their major customers, and the National CSIRT can create partner relationships that continuously improve security.

2.2.8 Academia

Educational institutions play a key role in developing the human capital and technical skills needed to solve complex problems, such as aspects of cyber security. Academics conduct research that enhances the technical, legal, and policy aspects of cyber security. In many countries, educational institutions have championed and hosted National CSIRTs.

2.2.9 Foreign Governments

Nations have a shared interest in mitigating cyber risk and working together to respond to incidents. Partnerships should be established to discuss global risk and interdependence as well as economic, political, and infrastructure concerns. Countries aligned with one another can exchange valuable intelligence and promote regional cyber prevention and preparedness.

---

[3] Definition according to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. no 107-56, section 1016(e).

2.2.10 Citizens

The citizens of a nation have a stake in the reliable performance of a nation's strategy for cyber security and are an inherent part of that strategy.

2.3 The Special Role of the National CSIRT

National CSIRTs react to computer security incidents deemed to be of national importance.[4] Because they collect and analyze information about computer security incidents on a daily basis, National CSIRTs also provide lessons learned and other information that can help stakeholders mitigate risk. National CSIRTs encourage meaningful national discussion about cyber security and awareness through their collaboration with private and governmental stakeholders.

The following section outlines the special roles of a National CSIRT. Not every organization will provide these services or have these capabilities. However, these roles typify the ways that a National CSIRT supports national cyber security.

2.3.1 Analyzing Computer Security Incidents to Identify Intrusion Sets

An intrusion set is defined as groups of computer security incidents that share similar actors or methods. Establishing that similar actors or methods are involved may require various analytical techniques. Determining that different attacks use the same method may involve questions of attack vector (for example, email and spoofed web pages), similarities across samples of malware, or the routing of stolen information (through specific proxy IP addresses, for instance).

Identifying intrusion sets is a refined version of the correlation analysis familiar to many computer security incident handlers. Generally, incident activity is grouped into different categories, such as criminal activity, activity conducted by other nations, or undetermined activity. This information and analysis can then be submitted to other national authorities for action, depending on the nation's security concerns and objectives.

National CSIRTs may use sensitive information from national intelligence or law enforcement organizations in this analysis. The use of this type of information can amplify the National CSIRT's work but requires strong trust relationships between the National CSIRT and the government, as well as robust information security measures.

2.3.2 Resource to the National Government on Cyber Security Issues

A National CSIRT can be a valuable resource to the national government on technical, policy, and legal issues relating to cyber security. It can advise the government on the suitability or security of systems the government plans to install or implement. In addition, the National CSIRT can assist government organizations with technical alerts and bulletins, best practices, and other advisories.

2.3.3 Assessing National Cyber Readiness and Crisis Management

The National CSIRT helps test and measure the nation's level of resilience to cyber attacks and crises. This assistance can take the form of providing technical support and analytical methods to plan and stage exercises or advising on the state of current cyber threats.

---

[4] The question of which incidents rise to the level of national importance is covered more fully in Section 3.3.1.

2.3.4 National Alert and Warning

Most of the existing National CSIRTs fulfill a national alert and warning function. This function involves alerting key national communities about problems ranging from specific software and system vulnerabilities to evolving criminal methods and malware threats.

2.3.5 Organizational CSIRT Capacity Building

National CSIRTs can help organizational CSIRTs in the nation by providing advice, training, best practices, or in some cases, staffing.

2.3.6 Trusted Point of Contact and National Coordinator

National CSIRTs frequently act as a trusted point of contact for the nation on cyber security issues. For example, national teams often handle requests from other countries or foreign organizations concerning malicious activity emanating from computers or systems within the nation. In a similar fashion, National CSIRTs frequently act as coordinators for domestic organizations attempting to resolve cyber security incidents with foreign connections. In this role, the National CSIRT does not typically analyze or resolve incidents itself, but rather directs organizations experiencing security incidents to information, services, or other helpful entities.

2.3.7 Building a Cyber Security Culture

The National CSIRT can help build a cyber security culture within the nation. Building a cyber security culture consists of many activities, including: awareness and education of private citizens on online risks, educating national stakeholders on the impact of virtual activities to their organizations, and the implications of their activities for cyber and information security.

3 Strategic Goals and Enabling Goals for Incident Management Capability

This section describes the strategic and enabling goals to consider when establishing a national computer security incident management capability. The information provides a hierarchy of goals needed to ensure support for the National CERT and align the National CSIRT with national cyber security strategy. The enabling goals are specific steps to meeting strategic goals. Four strategic goals are established for a National CSIRT:

1. Plan and establish a centralized computer security incident management capability (National CSIRT).
2. Establish shared situational awareness.
3. Manage cyber incidents.
4. Support the national cyber security strategy.

Strategic goals are essential, long-term requirements that help build the capacity to react to cyber incidents and enhance information and cyber security on a national level. Following each strategic goal are enabling goals. Enabling goals outline the more detailed considerations and activities needed to implement the strategic goals. The guidance available for each goal varies based on the maturity of the topic. Some subjects, like incident handling, have a robust history. Others, such as implementing national cyber security strategy through National CSIRTs, are emerging disciplines.

This document is not meant to provide specific "how-to" instructions. Instead, it highlights the unique requirements for building capacity in cyber incident management. Each strategic goal section concludes with a listing of additional references and training resources. These sources are not exhaustive but provide the reader with the next steps for both training and informational resources.

3.1 Strategic Goal: Plan and Establish a Centralized Computer Security Incident Management Capability (National CSIRT)

Before the first security incident can be managed, the capability itself must be established in some organizational form, such as a National CSIRT. Having a sole source or point of contact for computer security incidents and cyber security issues provides a number of benefits. A single organization presents stakeholders with a known source of information. A National CSIRT can also supply the government with a conduit for coherent, consistent messaging on cyber security issues. With a single National CSIRT, government departments have a source for technical information to support their individual functional areas. Finally, the National CSIRT can encourage the discussion about cyber security and facilitate international cooperation on this issue. In some nations, unique considerations may require multiple National CSIRTs or an incident management capability spread across several organizations. This document provides guidance regardless of the exact organizational form.

A National CSIRT capability should be established and operated according to certain core principles. These principles help leaders make decisions in the face of limited resources and complex problems. The core principles for the national management capability are:

- Technical Excellence: The National CSIRT's capability should be the best possible given the resources available. This is important because the National CSIRT strives to be a trusted leader in the nation on computer security issues. While striving for excellence may seem an obvious point, it has certain implications for building a capacity subject to resource constraints. It implies, for instance, a preference for providing one or two incident response services very well, rather than attempting to establish a range of capabilities without proper staffing or funding. The emphasis should be on technical competency.
- Trust: Almost by definition, a National CSIRT will handle information that is sensitive or potentially embarrassing to stakeholders. Trust must be earned and maintained. Properly handling and protecting confidential information is an important component to building and managing this trust.
- Resource Efficiency: Resource efficiency means using available resources effectively. This consideration is covered in more detail below, but it implies an ongoing evaluation of which threats and incidents are truly of interest to the National CSIRT's overall strategy as well as to the community it serves.
- Cooperation: The National CSIRT should cooperate as fully as possible with both national stakeholders and other National CSIRTs to exchange information and coordinate the solving of complex problems.

Chief to the National CSIRT's success are adequate sponsorship and resourcing. The Enabling Goals listed here are intended to help the sponsor of a national incident management capability build this capability in the most robust way possible. Consider the following enabling goals in planning and creating the national incident management capability.

3.1.1 Enabling Goal: Identify Sponsors and Hosts

The sponsor of the National CSIRT should identify other organizational sponsors and likely hosts. Other sponsors may bring additional funding and support to the National CSIRT project. Of course, a physical location, or host, for the National CSIRT must also be identified. In some countries the host is an academic institution. If hosted by a university, however, the National CSIRT may have difficulty obtaining the resources or authority it needs to interact with government stakeholders.

Various institutions and government departments may wish to support or host a National CSIRT. While any assistance is welcome, issues may arise when receiving support from certain stakeholders. Receiving sponsorship from an entity that is closely tied to a particular stakeholder or industry may limit the National CSIRT's perceived ability to service the entire community. This possibility should be examined, for example, if a specific for-profit enterprise operates a National CSIRT. In other cases, the involvement of certain sponsoring organizations may impede the willingness of key constituents to share information. Certain constituents, for instance, might be reluctant to share information if a regulatory or enforcement organization is the primary sponsor because of a concern that the information could be used against them.

3.1.2 Enabling Goal: Determine Constraints

The sponsor should determine which constraints may limit building and operating a National CSIRT. Typical constraints are budget, the availability of skilled staff, and the physical infrastructure available to support National CSIRT operations. For example, it might not be practical or desirable to build a malware analysis or deep packet inspection capacity in the National CSIRT. Limited constraints may dictate a more realistic approach is to build relationships with other domestic or foreign organizations that have this capability.

Constraints relate strongly to three of the core operating principles identified above: technical excellence, trust, and resource efficiency. Technical excellence requires a clear understanding of the staffing and budget available to support certain CSIRT activities. It may necessitate emphasis on a few core services performed well, rather than attempting to provide a broad array of services. Limited constraints can highlight the importance of incident management coordination, rather than completion of every incident management task in-house. Earning the trust of key constituents requires operational and staffing stability plus the ability to safeguard sensitive information, both of which are directly impacted by resource limitations. Finally, resource efficiency requires understanding what resources are available.

3.1.3 Enabling Goal: Determine the National CSIRT Structure

Based on its function in national cyber security, a National CSIRT can operate under a range of modes, including: an independent agency with limited operating partnerships, a joint operation with national telecommunications providers, or an integral part of the national military defense strategy. A number of factors must be considered to ensure detection and incident coordination and response are appropriately structured. The following list of structural considerations is meant to be exploratory and not comprehensive.

- What level of government directs the National CSIRT?
- Who funds the National CSIRT and who approves the budget?
- Is there an independent body that oversees the National CSIRT?
- What set of roles and responsibilities have been identified for National CSIRT operating partners?

There are several considerations that may be helpful in resolving the question of organizational form, in addition to the core principles.

- What structure would best allow the National CSIRT to alleviate potential stakeholder concerns with regard to sharing information?
- Are there any possible organizational structures that may limit the National CSIRT's perceived ability to serve its community in an unbiased fashion?
- Are the nation's systems and infrastructure already structured in ways that would make multiple National CSIRTs beneficial in terms of information sharing or reporting relationships?
- If multiple National CSIRTs are instituted, how should they share information? Is there a risk that multiple National CSIRTs may not be able to effectively share information across

infrastructure sectors? What are the transaction costs associated with having multiple organizations? How to they compare to the benefits of scale of a single National CSIRT?[5]

- Do the various possible organizational forms have any implications for staffing and managing human capital?

3.1.4 Enabling Goal: Determine the Authority of the National CSIRT

The National CSIRT proponent or sponsor should determine if the National CSIRT will have the authority to proscribe or mandate certain actions or security measures. The authority of a National CSIRT may differ based on whether it is addressing private citizens and industry or government departments. The National CSIRT or the sponsoring organization may have authority over various government departments but have no authority over private citizens.

These decisions should be consistent with the nation's law and culture. However, National CSIRTs are generally more effective when they act in an advisory role only. Major national stakeholders are often more willing and, depending on the legal environment, able to fully share information and discuss security vulnerabilities in a collaborative venue where the National CSIRT is not a regulatory or proscriptive body.

3.1.5 Enabling Goal: Determine the Services of the National CSIRT

The minimal essential function of a National CSIRT is the ability to respond to cyber security threats and incidents that are of importance to national stakeholders. The various National CSIRTs currently in existence execute a variety of functions. These functions include the typical roles of a National CSIRT[6] as well as services that typify organizational CSIRTs,[7] including

- Incident Handling Services
- Incident Analysis
- Forensic Services
- Network Monitoring Services
- Malicious Code Analysis
- Vulnerability Assessments

---

[5] A note about regional collaboration: The sponsor of a National CSIRT may consider sharing resources and costs with neighboring nations to form a regional computer security incident management capability, essentially a "Regional CSIRT." This may be an effective way to address the inherent problem of fulfilling many requirements with limited resources. A full examination of such an arrangement is beyond the scope of this report; however, there are compromises inherent in this solution.

Because one of the main functions of a National CSIRT is to reconcile the need to respond to global challenges with the nation's embedded law, culture, and national structure, the ability of a regionally-based CSIRT to provide value to multiple nations may become diluted. Secondly, because cyber security is part of a nation's overall security strategy, regional CSIRTs may often possess information that has important national security implications. A regional CSIRT may be limited in its ability to solicit this information from certain national stakeholders because of concerns about sharing this information in a multi-national venue. Sharing this sensitive information would require thoroughly anonymizing it. In any event, it would require a high degree of comfort and familiarity between nations, or an effective multi-national governance structure, for a regional CSIRT to be successful.

[6] Discussed on page 5.

[7] A full list of CSIRT services is available at http://www.cert.org/csirts/services.html

- Research Services
- Training Education Awareness
- Coordinating Response

These functions are limited by the constraints identified in enabling goal 3.1.2 (for example, funding, staffing, physical resources). The National CSIRT sponsor organization must determine which activities are realistic given the constraints. A particular National CSIRT often can best fulfill its role through close coordination with other National CSIRTs that possess greater technical capability or trusted communication channels.

3.1.6 Enabling Goal: Identify Additional Stakeholders

The sponsor of the national incident management capability should evaluate which other institutions may have input or interest in the establishment of a National CSIRT. A detailed list of the typical stakeholders in national cyber security policy appears in Section 2 of this document. Additionally, some stakeholders may be interested in taking a more active role in the formation and operation of a National CSIRT. Typically these include

- law enforcement
- technology vendors
- government users (government agencies, ministries, and so on)
- research communities
- governance bodies

The National CSIRT should understand how identified stakeholders complement and integrate into National CSIRT operations and develop a plan to incorporate bi-directional communication into its operations.

3.1.7 Additional Resources for Planning and Establishing a National CSIRT

The following is a list of publicly available resources for sponsors and champions considering the establishment of a National CSIRT.

Reference materials

- CERT® Program's Resource for National CSIRTs
  http://www.cert.org/csirts/national/
- CERT listing of National CSIRTs
  http://www.cert.org/csirts/national/contact.html
- Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?
  http://www.cert.org/csirts/csirt-staffing.html
- Resources for Computer Security Incident Response Teams (CSIRTs)
  http://www.cert.org/csirts/resources.html
- Defining Incident Management Processes: A Work in Process
  http://www.cert.org/archive/pdf/04tr015.pdf

® CERT is a registered mark owned by Carnegie Mellon University.

- Forum of International Response and Security Teams
  http://www.first.org
- Forums of Incident Response and Security Teams (FIRST) Best Practice Guide
  http://www.first.org/resources/guides/#bp21
- ENISA: Support for CERTs / CSIRTs
  http://www.enisa.europa.eu/act/cert/support
- ENISA: Baseline capabilities for National CSIRTs
  http://www.enisa.europa.eu/act/cert/support/baseline-capabilities

Training resources

- CERT Overview of Creating and Managing CSIRTs
  http://www.sei.cmu.edu/training/p68.cfm
- CERT Creating a Computer Security Incident Response Team (CSIRT)
  http://www.sei.cmu.edu/training/p25.cfm
- CERT Managing Computer Security Incident Response Teams (CSIRTs)
  http://www.sei.cmu.edu/training/p28.cfm

3.2 Strategic Goal: Establish Shared Situational Awareness

The essential function of a National CSIRT is managing cyber security threats and incidents of importance to national stakeholders. Excellence in incident management helps the National CSIRT build relationships with stakeholders and achieve other strategic objectives, such as supporting the national cyber security strategy. The first step in managing incidents is establishing an understanding or awareness of who the National CSIRT's major constituents are, what types of systems they employ (information and communications technology), and what types of incidents they experience. This general understanding of the environment is typically referred to as shared situational awareness.

Capable staff and exceptional technical infrastructure are wasted if the community is unwilling to inform the National CSIRT about incidents. Therefore, the first enabling goal focuses on trust.

3.2.1 Enabling Goal: Establish and Maintain Trust Relationships

National CSIRTs collect sensitive information about national constituents' problems, concerns, and vulnerabilities. They frequently use this information to derive lessons learned and publish informational reports, a process which carries the risk of revealing too much information if performed carelessly. National CSIRTs also disseminate general cyber security information to stakeholders. Building trusted relationships with stakeholders is essential to facilitating this two-way information exchange. Without the confidence of knowing that sensitive information will be adequately protected and compartmentalized, stakeholders will hesitate to share their sensitive information.

Ensuring the confidentiality of stakeholder information is an information security issue. It requires risk assessment at the National CSIRT level and implementation of the resulting recommendations. There are numerous codes of practices and frameworks available to help organizations such as a National CSIRT secure information. Regardless of the specific security measures and poli-

cies, the National CSIRT should proactively address stakeholder confidentiality concerns and be as transparent as possible about the security steps performed.

3.2.2 Enabling Goal: Coordinate Information Sharing between Domestic Constituents

One of the most important factors in establishing a national capability is to facilitate reliable and effective information sharing. A key role for a National CSIRT is to obtain incident information from the community and to disseminate timely and relevant response information back to the community. This type of information generally includes the following:

- incoming information about security incidents, collected through a variety of means
- security bulletins, awareness information on cyber threats and vulnerabilities
- general, specific, and urgent cyber warnings and alerts (technical and non-technical)
- best practices to prevent cyber security problems, events, and incidents
- general National CSIRT information (e.g., organizational chart, sponsorship, services provided by the National CSIRT, contact number/email address, etc.)
- resources and reference materials (e.g., security tools, partner organizations)

The information collected by the National CSIRT can reduce risk by supporting organizations subject to attack. This support may take the form of direct technical support, may involve working with third parties to find remedies and workarounds, or may involve raising awareness within industry. A key part of information sharing is that sensitive information from constituents may be shared only after being anonymized during the analysis process and in accordance with the National CSIRT's policies.

Anonymization requires sensitivity to specific circumstances, either involving computer security incidents themselves or the major constituents. For instance, a publicized incident report may redact the names of the victims or the constituent company involved. However, if it involves a notable incident discussed in the press, it may fail to actually protect confidences. A basic principle of protecting information is receiving the approval of the parties involved before releasing information or publicizing reports.

3.2.3 Enabling Goal: Integrate Risk Information from the Community

National CSIRTs benefit from open, shared information from private industry, academia, and government. When organizations conduct thorough risk assessments and share the results with the National CSIRT, situational awareness increases. Risk information from the community provides insight into the effects of security vulnerabilities and system problems, helping the National CSIRT to focus and refine its incident management process.

In its operational role of responding to incidents, a National CSIRT is a key contributor to situational awareness. By analyzing trends in the incidents being managed, the National CSIRT learns about the status of cyber security in the community it serves. The National CSIRT uses this knowledge and its own perspective on problems to produce a credible, realistic picture of national situational awareness. This helps the National CSIRT identify proactive defense strategies and needed improvements in community practices and behaviors.

3.2.4 Enabling Goal: Collect Information about Computer Security Incidents

A National CSIRT must be able to collect information about computer security incidents and events, receiving reports about suspected or confirmed incidents requiring coordination or response. National CSIRTs collect this information through two primary means: the trusted relationships they build and the technical infrastructure required to process incoming reports. While incident reporting is frequently voluntary and facilitated by trust, in some cases it may be mandated.

Capturing reports about computer security events and incidents requires the community to detect, identify, and track anomalous activity, employing both technical and non-technical methods. Anomalous activity is defined as activity that deviates from some establish norm of system operation. In many cases, collecting computer security incident information may first require educating communities about detecting this activity.

A key component of information sharing is maintaining tools, techniques, and methods that enable the National CSIRT to communicate with its community. Examples can include the following:

- a website for communicating and disseminating information—both general (publicly accessible) and sensitive (secure portal requiring authentication) between the CSIRT and its community
- mailing lists, newsletters, trends, and analysis reports
- implementation of secure information networks for CSIRT operations

3.3 Strategic Goal: Manage Incidents

A National CSIRT, acting as a trusted, national cyber security focal point, is uniquely situated to manage incidents of national concern. To accomplish this, many National CSIRTs establish certain active capabilities, such as incident response and containment, and service reconstitution. In many cases, the National CSIRT will not handle all of the incident handling and analysis itself. A National CSIRT may facilitate and coordinate analysis and response, either because of limited resources or because knowledge about the specific problem resides elsewhere, for instance at another National CSIRT or at a technology vendor.

3.3.1 Enabling Goal: Define Incidents and Threats of National Interest

Resources are scarce. Defining incidents and threats of interest to a National CSIRT is perhaps the most challenging task facing the National CSIRT. Determining where the National CSIRT should focus its attention is an iterative, evolving process. After the initial formation of an incident management capability, the National CSIRT typically is inundated with questions and requests for assistance. This places the National CSIRT in the position of having to balance the scarcity of time and resources with a desire to serve the community and build relationships with stakeholders.

While building the National CSIRT capability, several resources can assist the sponsor with defining the initial focus areas for the National CSIRT. These resources include the following:

- information systems and incidents that affect those critical infrastructure sectors identified in the National Cyber Security Policy, if there is one. This should be the primary initial driver

behind the National CSIRT focus areas. Providing guidance to the National CSIRT is one of the principal reasons for having a coordinated national policy.

- incidents and threats that may affect systems in one or more sectors of critical infrastructure
- types of incidents or activity that may be of unique concern to national authorities because they directly affect national security, reveal sensitive information, cause embarrassment to the nation, or because of other unique factors
- incidents that substantially affect a majority of computer users in the general public
- knowledge and experience of the National CSIRT's staff
- types of threats that are judged by the National CSIRT's incident analysts and the incident response community as part of greater or evolving threats
- knowledge and shared wisdom from other National CSIRTs

Awareness of the systems currently in use by the National CSIRT's key constituents can help the National CSIRT focus its analysis of incidents. This awareness is built over time through handling incidents and interacting with the community.

3.3.2 Enabling Goal: Analyze Computer Security Incidents

All National CSIRTs must respond to cyber incidents and provide the community with analysis and support. Not all National CSIRTs will have identical capabilities to do this work. For instance, not all National CSIRTs will have the same level of external partnership with information technology experts, software development communities, and security researchers. Nor will all National CSIRTs employ internal teams to perform code-level analysis of malware and software and to replicate attacks and exploits. However, at a minimum, National CSIRTs should analyze incident reports to discover shared characteristics, determine their importance, and accurately gauge the level of threat represented by the problem. Shared characteristics may include such things as attack vector and attack targets. In some cases, these shared characteristics may involve identifying or attribution information that can be useful to the nation's security services.

3.3.3 Enabling Goal: Develop an Efficient Workflow Process

A National CSIRT receives information from multiple sources about computer security incidents. These notifications come via email, web form, telephone, fax, or automated process (that is, event notification from automated information systems and sensors). Personal reports (those from individuals rather than information systems) should be expected from both known and unknown sources. Known sources include operating partners, information sharing networks, trusted members of private industry, government stakeholders, and significant domain subject matter experts (such as research scientists). Unknown sources may include reports from citizens and other organizations where a relationship does not exist. One example is the "hotline," which is a posted phone number or instant messaging service which allows parties to report incidents to the National CSIRT 24/7/365. These incidents vary by severity and importance.

To efficiently and fairly handle reports, a National CSIRT should establish a clear, consistent workflow process. Typical steps would include

- Detect events
- Analyze and triage events
- Declare incidents
- Respond to and recover from incidents
- Learn from incidents

3.3.4 Enabling Goal: Warn the Community

Timely notification of a threat can be the difference between proactively protecting systems and recovering them after an incident. Warnings and alerts increase the ability of the affected constituents to prepare for and detect threats and vulnerabilities, reducing the potential impact of risk. Warning the community about relevant problems will foster healthy relationships, promote practices for situational awareness, and provide evidence for the "value-added" benefit of a National CSIRT.

A National CSIRT uses its relationships with stakeholders and with other National CSIRTs, as well as its collected incident reports and analysis of those reports, to learn about threats and vulnerabilities and identify information that needs to be distributed to the community. A National CSIRT must design warnings to inform the community and encourage them to act to defend themselves. However the National CSIRT must balance the need to disseminate the information quickly with the sensitivity of the information and the format of the warning. Such warnings must be sent to the community in a manner that provides for its authenticity, integrity, and privacy where required. In addition, some warnings require confidentiality regarding the source of the information, particularly in cases where an intelligence source supplies threat information. Care needs to be exercised to ensure that while relevant threat information is effectively shared, it is not shared to those without a need to know. Many National CSIRTs remove information that may indicate the source of threat and vulnerability data, limiting communications to the vulnerability discovered or obscuring specific threat data.

Warnings from the National CSIRT to stakeholders and the national community in general are typically more effective when transmitted through trusted, confidential communications channels that have already been established. These channels may take the form of specific individuals or offices in key organizations. Working through pre-established, confidential communication mechanisms is a proven strategy for building trusted relationships. As a basis of the trusted relationships, National CSIRTs and their stakeholders and major constituents agree upon the communications method, the terms of information handling, and other protections. This enabling goal is closely tied with establishing trusted communications.

3.3.5 Enabling Goal: Publicize Cyber Security Best Practices

A National CSIRT collects information about security issues through various means, including its incident management process, the research it performs, and information sharing with communities and other National CSIRTs. Lessons extracted from multiple incidents can form the basis for targeted skills development and general security awareness. They also often improve situational

awareness and contribute to overall cyber risk management. A National CSIRT may communicate best practices through the publication of general cyber security best practice documents; guidance for incident response and prevention; training; recommended organizational procedures; and published case studies of practice adoptions. A National CSIRT may produce best practices about

- how to secure specific technologies against known attacks and cyber security threats
- how to develop, test, and exercise emergency response plans, procedures, and protocols
- how to coordinate with the National CSIRT on security research (e.g., vulnerability identification, root cause analysis, and threat and attack community research)

3.3.6 Additional Resources for Establishing Situational Awareness and Managing Incidents

The following is a list of publicly available resources for establishing cyber security awareness and managing incidents:

Reference materials

- CERT Resiliency Management Model (RMM)
  http://www.sei.cmu.edu/library/abstracts/reports/10tr012.cfm
- Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®)
  http://www.cert.org/octave/
- FIRST Papers & Presentations related to Computer Security
  http://www.first.org/resources/papers/index.html
- FIRST Best Practices Guides
  http://www.first.org/resources/guides/index.html
- ENISA Quarterly Review
  http://www.enisa.europa.eu/publications/eqr

Training resources

- CERT Assessing Information Security Risk Using the OCTAVE Approach
  http://www.sei.cmu.edu/training/p10b.cfm
- CERT OCTAVE Approach Instructor Training
  http://www.sei.cmu.edu/training/p42b.cfm
- CERT Computer Security Incident Handling Certification
  http://www.sei.cmu.edu/certification/security/csih/
- FIRST Network Monitoring SIG meetings
  http://www.first.org/meetings/nm-sig/
- Computer Security Incident Handling
  http://www.first.org/conference/
- CERT Virtual Training Environment
  https://www.vte.cert.org/vteweb/default.aspx

® OCTAVE is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. ℠Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

- FIRST Technical Colloquia & Symposia
  http://www.first.org/events/colloquia/
- SANS courses
  http://www.sans.org/security-training/courses.php

Materials on Warning the Community

- United States Department of Homeland Securty Stay Safe Online Website
  http://www.staysafeonline.org/ncsam
- United States' US-CERT repository of cyber security situational awareness information
  http://www.uscert.gov/
- US-CERT Vulnerability Notes Database
  https://www.kb.cert.org/vuls/
- National Institute of Standards and Technology: National Vulnerability Database
  http://web.nvd.nist.gov/view/vuln/search
- Australia's Stay Smart Online Alert Service
  https://www.ssoalertservice.net.au/
- United Kingdom's Warning, Advice, and Reporting Point's newsletters
  http://www.warp.gov.uk/Index/WARPNews/indexnewsletter.htm
- International Telecommunications Union's collection of Security Alert Providers
  http://www.itu.int/osg/spu/ni/security/links/alert.html

3.4 Strategic Goal: Support the National Cyber Security Strategy

A National CSIRT acts within a broader context of national incident management to monitor a host of diverse threats (for example, man-made and natural, physical and cyber). A National CSIRT can be used to

- determine additional national strategic requirements for cyber security
- identify needed technical practices, educational improvements, skills development of cyber security practitioners, and research and development
- identify opportunities to improve cyber security policy, laws, and regulations
- improve the measurement of damages and costs associated with cyber incidents

Perhaps most importantly for the national cyber security strategy, a National CSIRT can help promote a national culture of cyber security. By bringing together diverse groups, the National CSIRT can help stakeholders better understand security issues and the importance of these issues within their various communities.

3.4.1 Enabling Goal: Translate Experiences and Information to Improve National Cyber Incident Management and Cyber Policy Development

While organizations of all sizes will continue to perform internal cyber incident management, a National CSIRT alone has the primary responsibility of addressing national-level concerns. Translating National CSIRT experiences entails considering ways in which the National CSIRT's work and the experiences of the community may have broader implications for national laws and poli-

cies. This translation can produce lessons learned and improve risk mitigation nationally, as well as influence national regulations, guidance, initiatives, and directives.

Translated experiences may include incidents involving vulnerabilities in a system the national government is considering deploying across its departments, agencies, and ministries. Understanding the inherent risks may help determine whether or not to adopt a technology. Another example may involve ambiguity or inconsistency in privacy law that impedes information sharing among private stakeholders. The sources for these lessons learned include both the National CSIRT's experiences and the experiences of stakeholders.

3.4.2 Enabling Goal: Leverage Public Private Partnerships to Enhance Awareness and Effectiveness

Protecting critical infrastructure and cyberspace is a shared responsibility best accomplished through collaboration between government and the private sector, which often owns and operates much of the infrastructure. Successful government-industry collaboration requires three important elements: (1) a value proposition, (2) clearly delineated roles and responsibilities, and (3) bidirectional information sharing. The success of the partnership depends on articulating the mutual benefits to government and industry partners. The benefits to governments include, among others

- influence on the protection of national critical infrastructure not owned or operated by the government
- increased situational awareness through robust bidirectional information sharing

In assessing the value proposition for industry, benefits of working with government to enhance cyber security include

- access to actionable information regarding critical infrastructure threats
- increased sector stability that accompanies proactive risk management
- opportunity to influence related policy and initiatives

National CSIRT operational and strategic capabilities require active participation from all of its partners. Governments and industry should collaboratively adopt a risk management approach that enables government and the private sector to identify the cyber infrastructure, analyze threats, assess vulnerabilities, evaluate consequences, and identify mitigation plans. The capability of the National CSIRT to prioritize threats is also enhanced by the collaborative identification of privately owned critical infrastructure.

3.4.3 Enabling Goal: Participate In and Encourage the Development of Information Sharing Groups and Communities

The National CSIRT's participation in information sharing groups and communities is an important way to enhance situational awareness and build trust relationships. Information sharing in this context should ideally be bi-directional between the National CSIRT and its community. With regard to infrastructure operators specifically, incident and risk information should flow to the National CSIRT from industry, while the National CSIRT, in turn, disseminates threat, vulnerability, and mitigation information. Government, the National CSIRT, and industry can enhance this information flow by developing a formal framework for incident handling, including issues sur-

rounding information sharing. The framework should include policies and procedures for sharing information and reporting incidents, protecting and disseminating sensitive (government and industry) proprietary information, and mechanisms for communicating and disseminating information.

There are several different types of information sharing groups. Where the National CSIRT identifies a need for a particular venue in which to share information, it should take the lead in establishing such an organization.

Industry groups are comprised of separate firms in the same industry, for instance the several electrical suppliers in a nation. These groups can provide valuable information about vulnerabilities and incidents in a particular industry and can be productive venues to encourage discussion about cyber security. While industry groups are beneficial, participants may sometimes be reluctant to share proprietary or sensitive information with competitors.

Communities of interest are generally groups with a narrow, technology focus. These groups are integral components of information sharing because they often have deep technical knowledge, skills, and experience to study a problem and create solutions. Participants in these groups are often individuals recognized for their technical skills, leading researchers in the fields of cyber security and computer science, and private industry representatives from key information and communications technology providers (such as, infrastructure providers, software developers, and so on).

In some countries, communities of interest already share information on security threats, vulnerabilities, and impacts. Often, these groups also provide timely alerts and warning to members to facilitate efforts to mitigate, respond to, and recover from actual incidents impacting the critical infrastructures. Examples of these groups include Information Sharing and Analysis Centers (ISACs) in the U.S. and Warning, Advice, and Reporting points (WARPs) in the U.K.

Government-Industry working groups can greatly facilitate information sharing**.** Government can solicit comments from industry for cyber security policy and strategy development and can also coordinate efforts with private sector organizations through information sharing mechanisms. Government should ensure that the private sector is engaged in the initial stages of the development, implementation, and maintenance of initiatives and policies. Industry can benefit by gaining the opportunity to affect policy making and by learning how their sector fits in the overall national security picture.

Finally, the National CSIRT can play an important role organizing working groups among interdependent industries. Incidents involving one infrastructure sector can have cascading effects resulting in incidents in others, creating unanticipated interdependencies. For example, service disruptions in one public utility may create high volumes of customer calls, disrupting telephone networks. By developing an understanding of how cyber security affects multiple systems, the National CSIRT helps infrastructure owners and other organizations be sensitive to these interdependencies. Sharing information across infrastructure firms can facilitate the response to incidents across multiple sectors.

3.4.4 Enabling Goal: Assist the National Government in Responding to Incidents in Support of Government Operations

Where appropriate, the National CSIRT can enhance its role and effectiveness by handling incident response for government entities. Performing this role helps build trust relationships with government departments and helps the National CSIRT maintain an awareness of the systems and technology currently in use. In cases where incident response in specific departments is handled by an in-house CSIRT, for instance a CSIRT dedicated to the nation's armed forces, the National CSIRT can provide support by disseminating threat information and data from the nation's various organizational CSIRTs.

3.4.5 Additional Resources for Supporting the National Cyber Security Strategy

The following is a list of publicly available resources for understanding how National CSIRTs support a national cyber security strategy.

Reference materials

- DHS National Infrastructure Advisory Council: Reports and Recommendations
  http://www.dhs.gov/files/committees/gc_1227558980345.shtm
- US-CERT Government Collaboration Groups and Efforts to support government infrastructure
  http://www.uscert.gov/federal/collaboration.html
- National Council for Public-Private Partnerships (U.S.)
  http://www.ncppp.org/
- Partnership for Critical Infrastructure Security
  http://www.pcis.org/
- DHS Sector-Specific Plans
  http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
  http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
- CSIRTs and WARPs: Improving Security Together
  http://www.warp.gov.uk/Marketing/WARPCSIRT%20handout.pdf

4 Case Study: Selected Components of the National Policy on Cyber Security in the United States

Many government agencies help to formulate and implement cyber security policy in the United States. However, the Department of Homeland Security (DHS) is the lead agency for domestic incident management involving all types of critical infrastructure. The DHS Office of Cybersecurity and Communications provides crisis management in the face of significant cyber incidents, integrating information and helping to coordinate response across state, local, and federal government agencies as well as private industry. This role is part of the overall mission of DHS to protect critical infrastructure in the United States.

4.1 Critical Infrastructure and Key Resources

Homeland Security Presidential Directive 7 (HSPD-7) "Critical Infrastructure Identification, Prioritization, and Protection,"[8] identifies critical infrastructure sectors that the public and private sectors must work jointly to protect. While definitions may vary slightly, critical infrastructure (CI) is generally considered the key systems, services and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of those concerns. Critical infrastructure is composed of both physical elements (such as facilities and buildings) and virtual elements (such as networks and data).

The following eighteen CI/KR sectors have been identified in the U.S.

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Drinking Water and Water Treatment Systems
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare

[8] December 17, 2003, available at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

- Telecommunications
- Transportation Systems

4.2 The National Cybersecurity and Communications Integration Center

Because information and communications technology (ICT) supports almost all U.S. critical infrastructure sectors, cybersecurity is a major focus for DHS. The operational activities of DHS in support of national cybersecurity and communications CIKR are conducted by the National Cybersecurity and Communications Integration Center (NCCIC) in accordance with the National Cyber Incident Response Plan (NCIRP). The NCIRP is currently being updated with an interim version released in September 2010.[9] The NCIRP is based on and echoes principles in the preexisting National Response Framework of January 2008.[10]

The concept of operations for the NCIRP has two major components: the development and maintenance of a common operational picture and the concept of centralized coordination and decentralized execution of incident response activities. A common operational picture results in information being shared across a wide variety of public and private departments, agencies, and organizations. In other words, all major stakeholders in cyber security have a shared level of situational awareness. The common operational picture is created by the NCCIC.

The NCCIC is a 24/7 integrated cyber security and communications operations center that fulfils strategic goals common to National CSIRTs. NCCIC partners work together and are physically or virtually collocated to execute the National CSIRT mission. The NCCIC includes entities internal to DHS, such as US-CERT, as well as external partners like representatives from the military, U.S. federal law enforcement agencies, the intelligence community, and representatives from critical infrastructure sectors. The NCCIC acts to integrate information about cyber incidents from state, local, territorial, and tribal governments as well as open source information and incident information volunteered by private entities and companies. One of the challenges that characterizes this type of information exchange is how to appropriately share information in a way that both respects the concerns of parties providing the information[11] but also allows the information to be shared with enough detail to remain useful. To meet this challenge the NCCIC communicates across classified and unclassified channels and has institutionalized the appropriate standard operating procedures, channels, and portals to share information.

The second component of the NCIRP concept of operations is centralized coordination and decentralized execution. The U.S. relies on a decentralized ICT infrastructure that is owned by a variety of private firms and providers. In addition, the many components of the federal government—such as the military, civilian agencies, the Executive Office of the President, the Department of

---

[9] Available at http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf

[10] Available at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf. The National Response Framework details how the U.S. conducts an all-hazards response to incidents—from the smallest incident to the largest catastrophe. The National Response Framework identifies the key response principles, as well as the roles and structures that organize national response, laying the groundwork for first responders, decision-makers and supporting entities to provide a unified national response.

[11] These concerns may revolve around potential public embarrassment to the entity that experienced the incident or may involve fears that the incident information could disclose vulnerability data and be misused, causing more harm.

State, and others—each have their own legal roles and responsibilities. Governmental power in the United States is also shared between the federal government and state governments according to the U.S. Constitution. As a result, while the NCIRP seeks to centrally coordinate the activities and responses of these various entities, the actual execution of response actions takes place across many organizations.

The NCIRP separates cyber response activities into two categories, steady-state response and response to significant cyber incidents. Steady-state response means that the NCCIC is collecting and disseminating information about threats, incidents, intrusions, and vulnerabilities on an ongoing basis to build the common operational picture and enhance the situational awareness of NCCIC partners.

During response to a significant cyber incident, the NCCIC scales its operations to meet incident response objectives, adding additional staff if needed and communicating with all of its partners and stakeholders. The NCCIC's steady-state operations are structured so that in the event of a significant cyber incident, the NCCIC is already communicating with the same entities and people with whom it will need to communicate during times of emergency.

The National Cyber Risk Alert Level system (NCRAL) determines when a Significant Cyber Incident is occurring and categorizes risks to critical systems into four alert levels: guarded, elevated, substantial, and severe. The NCRAL level is determined by examining the observed or potential consequences of cyber threats, vulnerabilities, or events related to national security, public safety, the economy, public confidence, or combinations of these factors. The existence of these conditions is established through use of the common operational picture provided by the NCCIC, an examination of the potential consequences of cyber incidents, and the input of NCCIC partners, among other inputs. The NCCIC shifts into Significant Cyber Incident Response when the NCRAL level reaches the substantial or severe levels. The NCRAL "substantial" alert level occurs when there is "observed or imminent degradation of critical functions with a moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending." The "severe" alert level occurs when "highly disruptive levels of consequences are occurring or imminent."[12] While the NCRAL is not accessible outside of government, the United States Computer Emergency Readiness Team (US-CERT) maintains a similar National Cyber Alert System[13] that provides situational awareness about risk levels to the public.

4.3 United States Computer Emergency Readiness Team (US-CERT)

Created in 2003 by the National Cyber Security Division of DHS, US-CERT provides response support and defense against cyber attacks for the Federal Civil Executive Branch. This constituency consists of United States government civilian agencies that are part of the executive branch of government.[14] US-CERT also conducts information sharing and collaborates with federal, state, and local government agencies, industry, and the research community in order to dissemi-

[12] *National Cyber Incident Response Plan*, *Interim Version*, September 2010, page K-7, *available at* http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf

[13] Available at http://www.us-cert.gov/cas/alldocs.html

[14] This categorization excludes the United States military, for example, since the military is not a civilian agency, and the United States Federal Court system and United States Congress, as those are part of the judicial and legislative branches of government, respectively.

nate cyber security information to the public. US-CERT provides a communication channel for citizens as well as businesses and institutions, who are not already NCCIC partners, to coordinate and communicate directly with the United States government about cyber security incidents and concerns.

US-CERT:

- helps to manage incidents of national concern
- supports national cyber security strategy
- supports government operations
- serves as a trusted communications partner

US-CERT groups its mission responsibilities into three main categories:

- Information Sharing and Coordination: Informing national, state, and local government agencies, private sector partners, infrastructure owners and operators, and the public about current and potential cyber threats and vulnerabilities.
- Alert, Warning, and Analysis: Compiling and analyzing information about cyber incidents.
- Response and Assistance: Providing timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents.

The operational components of the US-CERT responsibilities can be detailed into five categories:

- Threat: Prioritization and mitigation
- Vulnerability: Prioritization, reducing attack surface and ensuring proper configuration
- Attack Detection: Early warning
- Mitigation: Preventing the attack
- Reflection: Changing policy, procedures, and technology to prevent reoccurrence

US-CERT produces a range of free, timely, and actionable information to improve the cyber security posture for all citizens. The National Cyber Alert System is an array of targeted communications operated by US-CERT to advise both technical and non-technical stakeholders. Technical Security Alerts and Security Bulletins provide detailed explanations of system vulnerabilities and recommended remediation. For instance, in March of 2009 US-CERT analyzed the Conficker/downadup computer worm and issued a diagnostic tool to help key communities determine if their systems were infected. Information and guidance were also provided to home users. US-CERT issues Security Alerts and Security Tips to convey vulnerability information to non-technical audiences. Federal agencies receive Federal Information Notices and periodic Trend Analysis Reports, and partners in private industry are provided Critical Infrastructure Information Notices.

5 Conclusion

There is a common need to resist, reduce, and fight cyber threats and respond to attacks. Instituting a national computer security incident management capability, such as a National CSIRT, is a valuable step towards helping nations manage this risk and secure their systems. Throughout this document, insight has been provided, which interested stakeholders and governments can use to develop a National CSIRT capability and determine its role within a strategy of national cyber security. Numerous resources have been included to allow the reader to obtain a deeper understanding of these cyber security issues and recognize the challenges facing National CSIRTs.

Nations seeking to manage cyber security risks are faced with key questions, such as, "How can a national incident management capability be built and maintained? How should a National CSIRT be integrated into government operations generally? How does the nation's legal and political environment affect national cyber incident management?" In the past, those seeking to build this capacity in their respective nations have looked to CERT or CSIRT organizations already in existence. While modeling existing organizations can be helpful in some cases, this approach also comes with problems. Existing CSIRTs are often the product of their own history, politics, or government. Building an effective incident management capability is often a much more nuanced process. It is hoped that this handbook can help leaders identify their own national solutions and build capabilities that best fit their nation's needs.

References

URLs are valid as of the publication date of this document.

[Brunner 2009]
Brunner, Elgin M. & Suter, Manuel. *International CIIP Handbook 2008/2009.* Zurich, Switzerland*:* Swiss Federal Institute of Technology Zurich, 2009.
http://www.css.ethz.ch/publications/CIIP_HB_08.

[DHS 2003]
Department of Homeland Security. *The National Strategy to Secure Cyberspace.*
http://www.dhs.gov/files/publications/publication_0016.shtm (2003).

[DHS 2008]
Department of Homeland Security. *National Response Framework.*
http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (2008).

[DHS 2009]
Department of Homeland Security. *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency*.
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (2009).

[Killcrece 2004]
Killcrece, Georgia. *Steps for Creating National CSIRTs.*
http://www.cert.org/csirts/national/ (2004).

[West-Brown 2003]
West-Brown, Moira; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin & Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002). Software Engineering Institute, Carnegie Mellon University, 2003.
http://www.sei.cmu.edu/library/abstracts/reports/03hb002.cfm

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	April 2011	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0, Version 2.0	FA8721-05-C-0003

6. AUTHOR(S)

John Haller, Samuel A. Merrell, Matthew J. Butkovic, Bradford J. Willke

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2011-TR-015

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-TR-2011-015

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

As nations recognize that their critical infrastructures have integrated sophisticated information and communications technologies (ICT) to provide greater efficiency and reliability, they quickly realize the need to effectively manage risk arising from the use of these technologies. Establishing a national computer security incident management capability can be an important step in managing that risk. In this document, this capability is referred to as a National CSIRT, although the specific organizational form may vary among nations. Nations face various challenges when working to strengthen incident management, such as the lack of information providing guidance for establishing a national capability, determining how this capability can support national cyber security, and managing the national incident management capability. This document, first in the *Best Practices for National Cyber Security* series, provides information that interested organizations and governments can use to develop a national incident management capability. The document explains the need for national incident management and provides strategic goals, enabling goals, and additional resources pertaining to the establishment of National CSIRTs and organizations like them.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Cyber security, incident response, national security	30

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL