Introduction

A cyber incident annex provides jurisdictions with a formal tool that outlines the capabilities necessary to effectively respond to and recover from a cyber incident.

The following section provides a cyber incident annex template that emergency managers may use to create their own jurisdiction-specific annex.¹

One appendix to the jurisdiction-specific annex may include implementation instructions in the form of maps, charts, forms, checklists, etc. In addition, we add two sample appendices to the template for consideration, as well.

¹ The template was created based on the 2013 National Response Framework (NRF) Cyber Incident Annex, and on the Wisconsin Cyber Incident Annex.
Cyber Incident Annex - [insert state/jurisdiction]

The [insert state/jurisdiction] Cyber Incident Annex aligns with the 2013 National Response Framework (NRF) Cyber Incident Annex. This Annex adapts concepts of the National Incident Management System to provide a systematic approach and standard set of principles to respond to a cyber incident with cascading physical effects. The Annex outlines the actions, roles, and responsibilities; governance structure; notification process(es); cyber incident definitions; and related authorities particular to a cyber incident.

[insert state] Coordinating Agencies

[List all state coordinating agencies in a cyber incident with physical effects. (e.g., Department of Administration/Division of Enterprise Technology, Department of Military Affairs/Division of Emergency Management)]

[insert state] Cooperating Agencies

[List all state cooperating agencies in a cyber incident with physical effects. (e.g., Department of Military Affairs/[state] National Guard, U.S. Department of Justice/[state] Statewide Information Center)]

Federal Coordinating Agencies

U.S. Department of Defense
U.S. Department of Justice

Federal Cooperating Agencies

U.S. Department of Commerce
U.S. Department of Energy
U.S. Department of Homeland Security
U.S. Department of State
U.S. Department of Transportation
U.S. Department of the Treasury
Intelligence Community
National Institute of Standards and Technology
Office of Management and Budget

I. Introduction

Purpose:
[Broadly describe the purpose of this annex (e.g., This Annex discusses policies, governance structure, actions, and responsibilities for a coordinated and multidisciplinary approach to prepare for, respond to, and recover from a cyber incident with physical effects.)

Scope:

[Describe which agencies and/or organizations should use this annex and which partners may work together.]

Policies:

[Describe the procedures and policies that govern the annex, specifically naming doctrine and entities involved in a cyber incident with physical effects.]

II. Concept of Operations

General:

[Provide a general background on the effects of a cyber incident with physical effects, the role of the [jurisdiction] government and their interaction with other levels of government, and definitions of a jurisdiction-wide cyber incident versus a national cyber incident, etc. In this section, also describe challenges and other cyber-related considerations for the response to and recovery from a cyber incident (e.g., the authorities of the federal government in cyberspace).]

Specific Responsibilities:

[Detail each coordinating and cooperating agency’s responsibilities in a cyber incident with physical effects.]

Organization:

[Identify and describe all entities involved in coordinating a response to a cyber incident with physical effects, including any and all interactions with cyber-specific partners. Also describe any additional cyber-specific entities and their roles and responsibilities. For example, if a state has a designated cyber response coordination group, then describe this group and its roles and responsibilities in a cyber incident.]
Describe and diagram the communication flow for interagency coordination for an effective unified command. Name and describe the responsibilities of the primary agencies, support agencies, and private-sector entities involved in a cyber incident with physical effects.

III. Actions

Steady-State:

[Name the state's/jurisdiction's pre-incident planning entities, and outline their ongoing planning efforts. Briefly describe the federal entities involved in cyber preparedness and in response to a cyber incident (e.g., the FBI's cyber crime entities).]

Notification and Activation Procedures:

[Name the specific state entity that will initiate the notification and activation process. Specifically, outline the notification process, including how information is shared, when information is shared, what information is important to share, and with whom the information is shared at the federal level and among the Information Sharing Analysis Centers (ISACs).]

Situational Awareness:

[List all state, federal, and private sources of information that may be used to inform situational awareness in an incident.]

Actions Following Notification:

[Specifically describe each entity’s actions that immediately follow notification of a cyber incident with physical effects. Name the entities that will assess and control the hazard. Outline how to identify and implement prevention and protection measures to address the threat. Also describe ongoing communication and coordination with federal entities and ISACs throughout a response, including when to report information, what to report, and how to report it.]

Short-Term Recovery Actions:

[Describe how to and who will implement short-term stabilization actions. What actions need to occur to continually monitor the cyber realm and recover from the physical effects? Identify how situational awareness is continued throughout recovery, and how resources are demobilized and/or re-allocated, etc.]
Appendix A: Authorities

State and Federal Laws:

[Insert any cyber-related state and additional federal laws, with a brief description of each. Some federal laws are provided below.]


Outlines assistance related to disaster preparedness and disaster response, mitigation, major disaster assistance programs, and emergency assistance programs.2

The Enhancement of Non-Federal Cyber Security, the Homeland Security Act (Section 223 of PL 107-296)

Outlines responsibilities of the Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection, and how coordination occurs with entities in crisis management.3

Federal Information Security Management Act of 2002 (FISMA)

Assigns responsibilities to various agencies to ensure the security of data in the federal governments. The act requires annual reviews of information security programs. “The Department of Homeland Security will exercise primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to the federal information systems that fall within FISMA under 44 U.S.C. §3543. In carrying out this responsibility and the accompanying activities, the Department shall be subject to general OMB oversight in accordance with section 3543(a), and the Department shall be subject to the limitations and requirements that apply to OMB under Section 3543(b)-(c).”4

Section 706, Communications Act of 1934, as amended 1996 (47 U.S.C. 606)

Section 706 of the Act provides the President with authority in a national emergency to control “any or all stations or devices capable of emitting electromagnetic radiations,” and in case of war or threat of war, to close “any facility or station for wire communication.” In terms of cyber, this essentially gives the President the power to shut down internet communications during a war or other kind of national emergency.5

---

3 http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf
4 http://www.dhs.gov/federal-information-security-management-act-fisma
5 http://www.house.gov/legcoun/Comps/FCC_CMD.PDF

Copyright © 2013 CNA Corporation
All Rights Reserved
Defense Production Act of 1950, as amended 2009
Allows the President to force the private sector to give priority to defense and homeland security for a limited period of time.\(^6\)

National Security Act of 1947, as amended 2007
Outlines the coordination for national security and information related to intelligence activities.\(^7\)


## Appendix B: Cyber Incident Definitions

### Sources of Cybersecurity Threats

<table>
<thead>
<tr>
<th>Threat Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bot-network operators</td>
<td>Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).</td>
</tr>
<tr>
<td>Criminal groups</td>
<td>Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.</td>
</tr>
<tr>
<td>Hackers</td>
<td>Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.</td>
</tr>
<tr>
<td>Insiders</td>
<td>The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.</td>
</tr>
<tr>
<td>Nations</td>
<td>Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.</td>
</tr>
<tr>
<td>Phishers</td>
<td>Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.</td>
</tr>
<tr>
<td>Spammers</td>
<td>Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).</td>
</tr>
<tr>
<td>Spyware or malware authors</td>
<td>Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.</td>
</tr>
</tbody>
</table>

---

Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

<table>
<thead>
<tr>
<th>Types of Cyber Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of incident</strong></td>
</tr>
<tr>
<td>Cross-site scripting</td>
</tr>
<tr>
<td>Denial-of-service</td>
</tr>
<tr>
<td>Distributed denial-of-service</td>
</tr>
<tr>
<td>Logic bombs</td>
</tr>
<tr>
<td>Phishing</td>
</tr>
<tr>
<td>Passive wiretapping</td>
</tr>
<tr>
<td>Structured Query Lange (SQL) injection</td>
</tr>
<tr>
<td>Trojan horse</td>
</tr>
<tr>
<td>Virus</td>
</tr>
<tr>
<td>War driving</td>
</tr>
<tr>
<td>Worm</td>
</tr>
<tr>
<td>Zero-day exploit</td>
</tr>
</tbody>
</table>