Global Information Assurance Certification Paper

Computer Network Defense at the National Level
Michael Tompkins
December 5, 2000

Purpose

This paper describes computer security organizations that are established and/or controlled at the national or international level for the purpose of protecting the critical infrastructure of the United States.

Background

The FY 1996 Department of Defense (DOD) authorization bill required that the President "report to Congress a national policy on protecting the nation's information infrastructure." [1] In response to this and other discussions on national security, the President established the President's Commission on Critical Infrastructure Protection (PCCIP) in July of 1996, which then released a report in October 1997. The PCCIP report was followed by Presidential Decision Directive No. 63 (PDD-63) in May 1998. Among other things, PDD-63 "sets a goal of a reliable, interconnected, and secure information infrastructure by the year 2003." [2] The National Infrastructure Protection Center (NIPC) was established as a result of PDD-63 and the directive encouraged the adoption of Information Sharing and Analysis Centers (ISACS) to be modeled after the Center for Disease Control and Prevention.

Introduction

The myriad of government-controlled and government-operated computer security organizations presents a virtual maze for security personnel to navigate. The individual who is new to the computer security business can quickly become overwhelmed with the list of organizations and their relationship to each other. I have attempted to explain many of the common governmental or quasi-governmental organizations and to describe their function and relation to other organizations. I have divided the organizations into four types or categories:

1. Federal Government Agencies (non DOD)
2. DOD Agencies
3. Partner Organizations
4. Federally Funded Research and Development Centers (FFRDC)

Federal Governmental Agencies (non-DOD)

"The Federal Computer Incident Response Capability (FEDCIRC) is sponsored by the Federal CIO Council." FEDCIRC is the central point of incident reporting for federal agencies when handling security incidents. [3] FEDCIRC day to day operations is run by CERT-CC and it is not intended to replace other incident response teams. FEDCIRC works with the NIPC for the planning of infrastructure protection strategies.

Another proposed program that resulted from PDD-63 is the Federal Intrusion Detection Network (FIDNet). FIDNet would be a multi-agency effort to connect Intrusion Detection Systems (IDS) from non-DOD federal agencies to FEDCIRC. It is important to note that FIDNet is not intended to monitor any private networks or require the installation of any new IDS systems. It is intended to operate from existing IDS systems and capabilities.[4]

The National Infrastructure Protection Center (NIPC) is the umbrella organization for all other non-DOD computer security organizations. The NIPC has an equivalent in DOD called the Joint Task Force for Computer Network Defense (JTF-CND). The NIPC is the focal point for gathering information on threats to infrastructure and is the main federal effort for coordinating incident responses, investigations, mitigation of attacks, and monitoring the reconstitution effort. [5]

NIPC maintains the InfraGard program, a grass roots effort started in Ohio, as part of their outreach effort. Eventually this program will expand to include all 50 states. This program provides four basic capabilities or services: local chapter activities, access to an Alert Network, access to a secure InfraGard website, and a Help Desk at the NIPC for InfraGard members. [6] The local FBI field office will assist members in identifying needs and concerns. Some of the activities a chapter might offer include seminars and conferences, education and training, a public website, and regular chapter meetings. InfraGard is organized around a geographical area and at this time almost all states have at least one chapter.

DOD Agencies

The DOD organization that is at the top of the flow chart is the Joint Task Force for Computer Network Defense (JTF-CND). As previously stated, the JTF-CND is equivalent to the NIPC in the non-DOD sector. The JTF-CND was formed in December 1998 and originally reported directly to the Secretary of Defense. In October 1999 it became a direct reporting command to Spacecom. During its first year of operation the JTF-CND reported over 22,000 attacks against DOD systems. Part of the JTF mission is to decide if the attack should be classified as a crime or a national security matter. Unless the attack is perpetrated by a foreign entity and the attack was launched from foreign soil it will be classified as a crime. [7] The JTF-CND is collocated with the Defense Systems Information Agency (DISA) Global Network and Operation and Security Center (GNOSC). This allows them to use the existing IDS capability.

DISA also includes the DOD-CERT. Their mission is to “protect, defend, and restore the integrity and availability of the essential elements and applications of the Defense Information Infrastructure (DII) under the full spectrum of conflict in support of the ‘Warfighter’.” [8] The major responsibilities of DOD-CERT give a clearer understanding of what they do. They serve as the technical advisor to the JTF-CND, coordinate responses where the JTF-CND is not engaged, and assess incidents reported by the various military regions and organizations.

Partner Organizations

The most important of the partnerships is the Information Sharing & Analysis Centers (ISAC). The creation of ISACS is encouraged by part of PDD-63. ISACs provide a way to gather, analyze and disseminate private sector information to the NIPC. The 50 – 75 banking and finance firms that agreed to form a limited liability corporation ISAC is one example. The telecommunications and the electric industries have also formed ISACS. [9] The mission of an ISAC is non-regulatory and non-law enforcement in nature. They are expected to have a high level of expertise available and to serve as a clearinghouse for information among sectors. ISACS appear to be somewhat similar to the InfraGard organizations, but ISACS are not geographical in nature. The 106th Congress introduced H.R. 4246 to address Freedom of Information Act (FOIA) and anti-trust concerns associated with ISACS.

The National Cybercrime Training Partnership (NCTP) has a mission to provide guidance and assistance to local, state, and federal law enforcement agencies to ensure that law enforcement is trained to fight high tech crime. This organization was developed by the U.S. Department of Justice in an attempt to deal with the fast pace of change regarding high tech crime and the specialized training required to combat cybercrime. [10]

Another partnership-type organization is the Forum of Incident Response Security Teams (FIRST). FIRST was formed in 1990 to address the need for better communication among incident response teams and security teams. The mission statement of FIRST says that "FIRST is an international consortium of computer incident response and security teams who work together to handle computer security incidents and to promote preventative activities." [11] Some of the goals of the organization are to share information and tools and to facilitate cooperation for effective prevention and detection of security incidents. FIRST is one of the oldest and best known of the .org sites. The list of partners is an impressive who's who list including Air Force Cert, Apple, AT&T, CIAC and many other academic and government groups. Other accomplishments of FIRST include the participation of CERT staff in FIRST's workshop on incident handling and having Wieste Venema as the current CEO and steering committee chairman.

Federally Funded Research & Development Centers

FFRDC's are organizations that assist the government with scientific research. The FFRDC that you will most frequently hear about is the Software Engineering Institute. The SEI was started in 1985 when the company won a competitive bid for government work and is operated by the Carnegie Mellon University. In 1988 CERT/CC was formed as part of SEI by the Defense Advanced Research Agency (DARPA). Originally, CERT/CC focussed on incident response, but since then they have expanded to include helping to start other incident response teams, coordinating efforts

of teams when responding to large-scale incidents, providing training, researching causes of vulnerabilities, and prevention of vulnerabilities. [12]

Contrary to what many people believe, CERT/CC has no connection to other groups with CERT in their name. CERT/CC may coordinate with them for incident response, but they are independent of these organizations. CERT/CC was a founding member of the FIRST.org and they are responsible for the day to day operations of the FEDCIRC.[13]

Endnotes

[1] Moteff, John D., "RL301153: Critical Infrastructures: Background and Early Implementation of PDD-63", September 12, 2000
Http://www.cnie.org/nle/st-46.html (12/5/00)

[2] "FACT SHEET PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES: PDD63, May 22, 1998
http://www.fedcirc.gov/pdd63faq.html (12/4/00)

[3] "Federal Computer Incident Response Capability"
http://www.fedcirc.gov/charter.html (12/4/00)

[4] "FAQ: Federal Intrusion Detection Network (FIDNet)"
http://www.fedcirc.gov/fidnet/fidnetfaq.html

[5] "Outreach", Information Sharing,
http://www.nipc.gov/infosharing/infosharing.htm (12/4/00)

[6] "Program Services", InfraGard,
http://www/nipc/gov/infragard/infragard.htm (12/4/00)

[7] Schaeffer, Richard C. Jr, "Computer Security: Cyber Attacks – War without Borders"
http://www.house.gov/reform/gmit/hearings/2000hearings/000726cybersecurity/000726rs.htm (12/4/00)

[8] DOD-CERT ONLINE
http://www.cert.mil/about/mission_statement.htm

[9] Moteff, John D., "RL301153: Critical Infrastructures: Background and Early Implementation of PDD-63", September 12, 2000
Http://www.cnie.org/nle/st-46.html (12/5/00)

[10]About NCTP
http://www.nctp.org/about.html (12/5/00)

[11] "FIRST Statement of Mission and Strategic Goals"
http://www.first.org/about/mission.html (12/5/00)

[12] About the CERT/CC
http://www.cert.org/nav/aboutcert.html (12/4/00)

[13] The CERT Coordination Center FAQ
http://www.cert.org/faq/cert_faq.html (12/4/00)

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event