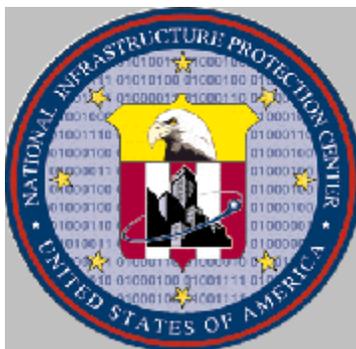


NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.



**Issue 5-01
May 15, 2001**

Editors: Linda Garrison
Martin Grand

-
- ! U.S. Water Industry: Potential Concerns Surrounding Consolidation**
 - ! Cracking by the Numbers: New Threat Posed by Exploit Programs**
 - ! Information Sharing and Analysis Centers**

For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or (202)323-3204.

We welcome your comments and suggestions for improving this product. To provide comments, contact the Editors at (202) 324-0334 or (202) 324-0353.

This issue has an overall classification of "Unclassified." This publication may be disseminated further without express permission.

U.S. Water Industry: Potential Concerns Surrounding Consolidation

Consolidation will inevitably result in changes in company operations for water suppliers that could impact the reliability or security of the water supply in affected areas .

Regulatory authorities have taken steps to encourage consolidation, especially in the case of water suppliers so small they may be unable to invest in the infrastructure necessary to deliver safe, reliable drinking water.

Recent Consolidations

- Philadelphia Suburban Corporation (PSC), one of the largest water companies in the U.S., has purchased nearly 40 water or wastewater companies since 1992.
- Acquarion, one of the ten largest private water companies in the U.S., has been purchased by the Kelda Group, a major United Kingdom (U.K.) water services company.
- Thames Water, the largest water company in the U.K., finalized its acquisition of E'Town Corporation, the seventh-largest water company in the U.S.
- United Water Resources, America's second-largest privately held water services company, was purchased by the French company Suez (formerly Suez Lyonnaise des Eaux), which is one of the largest providers of water services in the world .

Increased Automation

The acquisition of small, resource-poor water utilities by larger entities may result in greater levels of automation being introduced into operations. Water companies active on a regional scale may deploy remote monitoring and control systems. Steps should be taken to ensure that these automated systems are secured to prevent malicious intrusion or manipulation that could affect operations or water quality.

Personnel Restructuring

Consolidation typically involves restructuring in terms of personnel. The situation in the water industry where the restructuring displaces ultimate control from local management to a corporate structure located in another city or even another country is a factor that is likely to increase staff alienation. Management will need to take steps to minimize the danger from malicious insiders. In addition to prudent human resource management techniques, technical measures such as appropriate access controls and the timely termination of inactive computer accounts will be necessary.

Security Policy Integration

Corporate security policies should be promulgated to newly acquired facilities, which because of their small size may not formerly have had a well-developed formal security program in place.

Foreign Ownership

To date, much of the international commercial activity has involved companies from friendly, democratic countries. In the future however, the issue of foreign ownership of our drinking water infrastructure, one of our most precious and vital services, may become a question for society as a whole to consider.

Cracking By the Numbers: New Threat Posed by Exploit Programs

The availability of easy to use, pre-coded exploit scripts on the Internet has enabled novices to pose a serious threat by lowering the bar on the skills required to employ malicious code.

Many web sites appear to cater to beginners by including "How To's" and "FAQs" that provide detailed instructions, to teach would-be crackers step-by-step methods for exploiting computers. Rather than forcing a beginner to gain command line knowledge, the only skill set needed is the ability to point and click a Graphical User Interface (GUI). Teenagers with basic computer skills who initiate many of these attacks are often dismissed because of their age and lack of skill. Yet they possess the malicious intent to use tools written by more capable hackers and should be taken seriously, as these relative beginners have perpetrated some of the most widely reported cases of Internet crime.

One example of a relative novice using pre-coded exploits was that of Mafiaboy, a Canadian teen that launched the distributed denial of service attacks against several high profile websites. The tools used for these attacks are widely available on the Internet and require little computer knowledge to use. Indications that Mafiaboy was a fairly unskilled attacker included the fact that he failed to take basic steps to cover his tracks (such as erasing logs). This, however, did not stop him from successfully shutting down a number of prominent websites.

Viruses

Computer viruses don't require significant expertise to cause significant damage. The Kornikova virus, which recently proliferated throughout the Internet, was created with a pre-coded virus toolkit. Basic computer skills are generally all that is needed to use these toolkits, particularly when combined with effective social engineering.

Exploit Programs

Exploit programs also increase the workload on network security personnel. The unprecedented amount of time spent scanning for a program such as SubSeven, might force system administrators to focus on the scanning activity and distract them from a more serious attack.

The issue of web sites providing malicious code is certain to be a matter of contention in the future. In addition to the damage caused by the code, such sites enable individuals to hone their skills and become more proficient at these questionable activities. An alternate viewpoint is that making these programs easily available allows security engineers to access them in order to understand how they work and to develop counter measures. Having such programs publicly available may be preferable to the alternative of having them exchanged covertly in underground on-line chat rooms.

Information Sharing and Analysis Centers

Originally called for by Presidential Decision Directive (PDD)-63 in May 1998, Information Sharing and Analysis Centers (ISACs) are at various stages of development today.

ISAC Creation:

“The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government.”

ISAC Operation:

“Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government.”

The Business Case for ISACs

Encouraged by PDD-63, a number of private sector infrastructure entities have taken steps to establish ISACs (see Table 1). As with all business decisions, becoming a member of an ISAC involves a cost, benefit, and risk tradeoff. Some of the important membership *benefits* are:

- Members receive early notification of significant incidents and protection solutions, furnished focused information on the industry-specific threats, vulnerabilities, remedies; they may submit anonymous information to protect proprietary interests.
- Through the sharing of information, members are contributing to their own security, as well as to that of the other members of the ISAC sector; the resulting benefits will be to strengthen public confidence and goodwill, and to increase profits and market share.
- By reporting incidents, vulnerabilities and threats, members are enabling the early recognition of national trends and relationships, thereby contributing to the national security. NIPC can access the resources of the national defense, intelligence, and law enforcement communities, and is the premier instrumentality of the United States Government to assist infrastructure owners and operators in defending against cyber and physical attacks.
- Participation in an ISAC is an indication of due diligence in seeking to achieve and maintain good security in an era of increasing litigation.

Status of ISACs by Sector

A summary of the status of ISACs by PDD-63 sector and NIPC's relationship with them is presented in Table 1 below.

Table 1. Overview of ISACs

PDD-63 Infrastructure	ISAC Owners/Operators	ISAC Location/ Contact Information	Status
Electric Power	North American Electric Reliability Council (NERC) Eugene F. Gorzelnik efg@nerc.com , Louis G. Leffler, lou.leffler@nerc.com	ES-ISAC Princeton, NJ www.nerc.com/~filez/cip.html	Operational since October 2000; NERC CIP Working Group guides and oversees operations.
Information & Communications	National Coordinating Center (NCC) for Telecommunications	NCC-ISAC Arlington, VA; www.ncs.gov/InformationPortal/portal.html	Operational since January 2000; interim Information Sharing & Analysis System (ISAS) operational.
	Information Technology-ISAC, LLC./ Internet Security Systems (ISS) operating contractor	IT-ISAC Atlanta, GA; www.iss.net pallor@iss.net	Established on January 16, 2001.
Banking & Finance	Financial Services Information Sharing and Analysis Center Global Integrity Managed Services practice of Predictive Systems, Inc.	FS-ISAC Reston, VA www.fsisac.com 888-660-0134 for membership information	Operational since October 1999; Information shared within sector only.
Transportation	Association of American Railroads (AAR)	'Railroad Transportation' ISAC (TBD) Washington, DC www.aar.org Tel 202-639-2401 Fax 202-639-2526	Railroad ISAC established first; may be followed by Surface Transportation ISAC.
	U. S. Department of Transportation plans to pursue establishment of an Aviation ISAC	'Aviation'-ISAC (TBD)	Candidate organizations for becoming ISAC are being contacted.
Water Supply	The Association of Metropolitan Water Agencies (AMWA)/ Water Sector CIP Advisory Group established on December 12, 2000	'Water-Sector' ISAC (TBD) Washington, DC Tel 202-331-2820 Fax 202-785-1845 www.amwa-water.org	ISAC to be established upon EPA/Advisory Group study completion.
Oil & Gas	National Petroleum Council (NPC)/ Oil & Gas ISAC Working Group established	'Oil & Gas ' ISAC (TBD) Washington, DC Tel 202-393-6100 Fax 202-331-8539 info@npc.org ; www.npc.org	Working Group plans to recommend an ISAC on June 6 th to NPC.

PDD-63 Infrastructure	ISAC Owners/Operators	ISAC Location/ Contact Information	Status
Emergency Fire Services	US National Fire Academy; US Fire Administration; Federal Emergency Management Agency (FEMA)	'Emergency Fire Services'-ISAC (TBD); Emmitsburg, MD Tel 301-447-1117 Fax 301-447-1173 Usfacipc@fema.gov	USFA will serve as ISAC for 33,000 plus local fire & rescue departments.
Emergency Law Enforcement	NIPC Watch and Warning Unit (WWU) and the Emergency Law Enforcement Forum; also Sector Coordinator at sullivan@csn.net www.co.arapahoe.co.us/sh/	'Emergency Law Enforcement Services'- ISAC (TBD); NIPC WWU Nipc.watch@fbi.gov	Operational; using the National Law Enforcement Telecommunications System (NLETS) for Federal, State, & Local law enforcement communications.
Public Health Services	Department of Health and Human Services (HHS), Sector Liaison Agency wclark@os.dhhs.gov	None established	Formative planning stages.
Continuity-of- Government Services	Federal: FEMA, General Services Administration (GSA)	Federal: Federal Computer Incident Response Center (FedCirc) www.fedcirc.gov fedcirc@fedcirc.gov	Operational since October 1999.
	State: None	State: None	State: Both National Emergency Management Association (NEMA) (www.nemaweb.org) and National Association of State Information Resource Executives (NASIRE) www.nasire.org are considering ISAC question.

Further Information

As the first article in a forthcoming monthly series, this article provides an overview of the status of all ISACs established under PDD-63. Subsequent monthly articles will provide more details on individual ISACs.

The NIPC invites national associations, industry alliances, and other industry groups who feel that their membership could benefit from participation in an ISAC to contact the ISAC of interest as shown in Table 1. Alternatively, Mr. Paul Rodgers may be contacted at the NIPC at (202) 324-0341 or by email at prodgers@fbi.gov.