Title: Lessons Learned in Establishing a Virtual Computer Incident Response Capability

Chair:
Marianne Swanson, National Institute of Standards and Technology

Panelists:
Marianne Swanson, National Institute of Standards and Technology

Kathy Fithen, CERT/CC, Software Engineering Institute, Carnegie Mellon University

David Adler, General Services Administration

Abstract:
In October 1996, the National Institute of Standards and Technology (NIST) formally announced the creation of the Government Information Technology pilot project, "Federal Computer Incident Response Capability (FedCIRC)". On October 1, 1998, the FedCIRC project is transitioning from a successful pilot to a mature, operational service operated by the General Services Administration. The lessons learned in establishing and operating a virtual response team for the United States federal civilian agencies will be presented. Under NIST's direction two established incident response teams banded together to support all federal civilian agencies. The communication, coordination, and cooperation needed between the two teams will be shared.

The panel will also present some of the practical lessons learned while assisting agencies in establishing their own capabilities. FedCIRC was faced with the reality of agencies lacking funding, personnel, and equipment to carry out additional duties such as incident handling. For agencies to implement the requirements of OMB Circular A-130, innovative methods were needed. This panel will share some of the successful methods agencies have started to use.

The General Services Administration will present the new FedCIRC. How the capability differs from the pilot project and how to best work with the team will be explained.

Panel Statements:

Kathy Fithen
Lessons Learned – Communication, Coordination, and Cooperation
A virtual coast-to-coast incident response team consisting of two operational teams working together across large distances was challenging. The CERT/CC at Carnegie Mellon University and the Computer Incident Advisory Capability (CIAC) at the Department of Energy's Lawrence Livermore National Laboratory brought distinct but complementary technology and management experiences to FedCIRC. The presentation will share the coordination established between the teams – what worked and how it

could work better, the secure communication required and the cooperation needed to make the virtual team run smoothly.

Marianne Swanson
Lessons Learned in Establishing and Incident Handling Capability
The computer security effort at most agencies has already handled some network and system intrusion attempts and is therefore not naive to the issues involved in handling computer security incidents. The functions that comprise an incident handling capability are generally not new, though the coordination among the functions to act promptly and in unison when an incident occurs is. This presentation will discuss the more traditional computer security components that exist and show how these components easily lend themselves to an incident handling capability.

David Adler
Federal Computer Incident Response Capability (FedCIRC)
The FedCIRC is currently transitioning from a pilot to an operational program. The new FEDCIRC will be a collaborative partnership of computer incident response, security and law enforcement professionals who work together to provide assistance and guidance in incident response and handling across agency boundaries. FEDCIRC will foster communication among Federal agencies regarding computer incident prevention, detection and handling. Provide alert and advisory information regarding potential threats and emerging incident situations. FEDCIRC will also facilitate the sharing of security related information, tools, and techniques.