Jeffrey James Bryan Carpenter

4885A McKnight Road, PMB 503, Pittsburgh, PA 15237-3400 / +1 218 837-6000 / jjc@pobox.com

Sep 00 to Present: Technical Manager of CERT Coordination Center, Software Engineering Institute, Carnegie Mellon – Managed a technical program of operational analysis and applied research work including vulnerability, incident, network traffic, and malicious code analysis, creation of Computer Security Incident Response Teams (CSIRTs), and secure coding. Grew and managed the group from 10 to 32 employees ($4M to $12M/year budget) that is focused on working with industry, government, and academia to protect national and economic security and critical infrastructure by helping technology managers better protect their IT assets and manage cyber security risk. Conducted technical analysis of incidents and vulnerabilities.

• Led the team that created the National Cyber Alert System in 2003 for the Department of Homeland Security.

• Negotiated a three-year, $23 million contract with the DoD to support the DoD/Defense Industrial Base Collaborative Information Sharing Environment program designed to share incident and threat information with defense contractors to better protect DoD sensitive but unclassified information from our adversaries.

• Created the malicious code analysis team to develop tools, techniques, and training to make reverse engineers more effective and promote collaboration amongst those in the reverse engineering community.

• Created a vulnerability discovery program to develop tools and techniques vendors can use in Q/A processes to reduce vulnerabilities, and to increase collaboration in the vulnerability discovery community.

• Assisted numerous countries in the creation of and thought leader for National CSIRTs. Created the phrase and concept, "CSIRT with National Responsibility" to describe a capability a nation or economy needs to protect national and economic security and critical infrastructure by managing the risk from cyber threats.

• Created and hosted five workshops to share tools and solutions unique to National CSIRTs that were attended annually by approximately 70 technical staff representing 30 countries.

• Conducted hundreds of news media interviews and frequent public speaker including Congressional testimony.

Jan 98 to Sep 00: Incident Response Team Leader, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon – Led team of 8 incident responders managing an analysis workload of 2500 incidents per year. Taught tutorials and conducted site security evaluations. Developed innovative incident analysis models. Managed CERT/CC response to major internet security events.

• Led incident response efforts in creating and operating FedCIRC, the CSIRT for U.S. Government prior to the creation of DHS.

• Created and implemented Y2K incident response plan.

Sep 95 to Jan 98: Internet Security Analyst, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon – Provided technical analysis and advice to organizations reporting incidents to the CERT/CC. Reviewed submitted data including network and system logs, advised on how to determine what happened, how to recover, and how to prevent further attacks. Authored CERT Advisories and other documents on current incidents, vulnerabilities, and threats based on reporting and analysis.

• Rewrote tools used to manage incident reports and analysis.

Apr 88 to Aug 95: Systems Analyst, University of Pittsburgh Computer Center – Managed central network services including email, DNS, authentication and file service, overseeing a team of five system administrators. Responsible for needs and capacity planning. Conducted investigations into security problems including serving as a liaison with other organizations and law enforcement. Evaluated the security exposure for services.

• On a team that developed a distributed architecture used to manage software installation and maintenance on UNIX systems with minimal staff. It managed servers providing network services, desktop computers, and computing lab computers.

• Initiated security bulletin service for university system and network administrators.

Jan 10 to Present: President, Berkeley Hills Fire Company – Managed business affairs of a suburban fire company with 50 members, five pieces of apparatus, over 1200 calls per year, and an annual budget of $250,000.

• Instituted long-term planning process for budgeting and capital purchasing.

• Managing the funding and purchase of $900,000 ladder truck.

May 86 to Present: Firefighter/Fire Police Officer, Berkeley Hills Fire Company – Life member providing public service as firefighter, fire police officer, and member of board of directors.

BS Computer Science, University of Pittsburgh, 1989

Other Interests: Technology, telecommunications, amateur radio (W3JJC - amateur extra), parliamentary procedure, reading, British political history.