Prepared Statement of

Martin C. Faga
Executive Vice President
The MITRE Corporation

202 Burlington Road, Bedford, MA 01730
1820 Dolley Madison Blvd, McLean, VA 22102
703-883-1340
www.mitre.org

before the

Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
United States Senate

Hearing on Cyber Security and Critical Infrastructure Protection

March 1, 2000

I'm Marty Faga, the Executive Vice President of the MITRE Corporation and the Director of MITRE's C3I FFRDC. My testimony this afternoon addresses a single proposition:

> **To deal with emerging threats to our information infrastructure, of which the recent e-commerce attacks are only a precursor, we need to leverage the knowledge and experience of the Department of Defense and the broader national security community**.

MITRE has been working issues of computer network security for more than 30 years. We have some 450 technical staff providing cyber-security support to a wide variety of Government agencies and activities, particularly the Department of Defense and many of its Agencies, all the Military Services, and the Intelligence Community. My testimony today draws upon what we have learned over many years of supporting these information security activities.

We have all had our attention heightened by the recent denial of service attacks. While there are new tools such as TFN (believe it or not, Teletubbies Flood Network) that make these attacks more powerful and easier to launch, denial-of-service attacks are nothing new. What is new is that these targets are high-profile e-commerce sites. As the Internet becomes increasingly important to our economy, its vulnerabilities--even to relatively unsophisticated attacks--become increasingly significant. But I'm more concerned about the sophisticated, dynamic attacks that are technically possible today and increasingly likely to occur in the future. I say this because we do it--we mount sophisticated, professional cyber attacks in exercises so that we can learn about the challenges that defenders face. And we know from both classified and open sources that others are working on such sophisticated attacks as well.

While I will focus my remarks today on information system security, I am also concerned about the broader range of technology vulnerabilities that can affect our critical infrastructure: vulnerabilities in the wireless communication media on which we are increasingly depending; vulnerabilities in the systems that control our energy generation and distribution; and vulnerabilities in the global positioning satellite system, on which our infrastructure is increasingly depending for critical timing as well as positional information.

Experience Is Essential

In the cyber security arena, experience is critical. DoD, with partners such as MITRE, has been addressing cyber security problems for decades. It was in 1969 that MITRE, working together with the Air Force, demonstrated the vulnerability of an operating system to a cyber attack. DoD is currently developing and implementing plans to counter the information warfare threats waged by a technologically sophisticated enemy while it is under constant attack by hackers of varying degrees of skill. Over time, DoD and

MITRE have devoted a great deal of attention to issues of cyber security, and we have built up a very large base of experience. Some of the things we have learned include:

- **The value of the classical "warrior mindset" for planning a defense against an intelligent, adaptive, enemy.** This includes the assumption that the threat is dynamic rather than static -- that the enemy will always try to overcome our defensive innovations. It also includes making use of simulations and "red teams" to understand how our systems appear to an intelligent and committed enemy. Finally, it includes the concept of defense in depth: rather than setting up a single barrier to attack, we examine the full range of techniques that an attacker might use against us, and then we attempt to frustrate all of them.

- **We must approach cyber security as if we are in a never-ending "arms race" between the technology of cyber defense and the technology of cyber attack.** Just as every advance in tank armor stimulates a search for more effective anti-tank weapons, and every new tank-killing technology stimulates a search for better protection, cyber defenses are ultimately devised to thwart almost every cyber attack. Conversely, each new cyber defense technology is eventually overcome by cyber attack techniques. Even if we had perfect cyber security today, we would still have to face a new threat next week or next month that would prevail in the absence of additional or improved security innovation.

- **Security must be designed into information systems from the beginning, not added as patches.** Systems must be designed to be inherently more secure, with redundancy, diversity, and an ability to gracefully degrade built in. The cost of doing it right at the beginning of a program may appear to be expensive--indeed, even unaffordable. But the costs of dealing with the resulting vulnerabilities are much greater in the long run. The lesson, which should be applied to all future civilian and DoD information systems, is that every new information system and every major modification needs to budget for security as well as for functionality.

- **Cyber security requires an end-to-end systems approach with intense continuous attention to seemingly small details.** Among these details are the configurations of the myriad components that comprise our complex systems. Many commercial products, though they can be configured securely, are insecure "out of the box." They need to be configured properly to eliminate vulnerabilities. Furthermore, there are many cases in which two secure components or systems have been connected to each other in a way that creates new vulnerabilities.

- **Our defense must become more proactive.** Though the DoD and infrastructure providers are becoming more skilled and reacting to threats when they occur, we should be predicting future likely threats and developing

defenses in advance. This requires an ongoing analysis of current and emerging threats, and predictive analysis of future threats. To be most effective, the analysis needs to be based on both open and clandestine sources, and must include the expertise of the infrastructure operators. So the DoD and the broader national security community, as well as the private sector, should be partners in this enterprise.

- **We must make less information about the internal operation of our critical infrastructure systems public.** Details about how critical systems are wired together *internally* and how they are operated during times of crisis are among many facts important to an attacker. The less we enable the attackers, the better.

- **We must never assume that our systems are invulnerable.** An important part of our defense strategy must include a focus on systems that can gracefully degrade when under attack. We must also pay attention to backup, recovery, and reconstitution procedures.

- **Long-term research is needed to develop more proactive defenses.** Defense technology today largely defends against attacks of which we are aware. In the long term, we must improve our ability to defend against attacks we have never experienced before.

- **Training is critical**. Vulnerabilities arise when people are not adequately educated in proper security procedures and techniques. Examples include system administrators who do not understand how to secure their networks and individual users who do not understand the proper use of passwords. The vulnerabilities that arise from inadequate training are far more costly than the training itself.

The security of the US civilian information infrastructure would be enhanced by drawing upon what DoD has learned over the years. No other sector matches DoD's experience in defending information networks. DoD does not have to own the problem or the networks to have responsibility for being part of the solution.

Challenges to Information Sharing

This leads me to a second critical area -- information sharing. The National Plan for Information Systems Protection calls for more information sharing, and at first glance this sounds rather like apple pie – everybody ought to be in favor of it. MITRE believes that information sharing is indeed essential, but our experience has shown us that it is also very difficult. There are several reasons:

- While Government and industry clearly must work together, our democracy is founded upon a private sector that keeps a healthy separation from

government, and a government that regulates the playing field without trying to participate in the game.

- Sharing needs to be balanced against concerns of privacy and the basic structure of a market economy. An enterprise is unlikely to seek the help that it needs if the cost is the uncontrolled exposure of its internal affairs. Competition is the engine that drives most innovation in the United States, and to be effective, it often requires the protection of proprietary research and proprietary products.

- There is a dilemma about how much information to share, and with whom. If information about attacks and vulnerabilities is made freely available, then the attackers can and will make use of this information to design better attacks. If information about attacks and vulnerabilities is restricted to a tight circle of trusted insiders, then many organizations and enterprises will fall victim to attacks that they could have prevented. DoD has struggled over the years with the conflict between the need for awareness and the need for compartmentalization. We believe that this experience shows that rather than setting hard and fast rules, the process of information sharing must be flexible and sometimes subtle, constantly modifying existing practices to take advantage of lessons learned from experience.

- Effective sharing requires an effective catalyst. The model of sharing in which a single organization collects information from everybody and distributes it on a need-to-know basis will not work. There is no incentive for enterprises to share their experiences and their vulnerabilities when there is no assurance of receiving the help they need when they believe they need it. A central organization should act as catalyst and facilitator to help enterprises share with each other, but should not be the sole repository of shared information.

DoD and the civilian infrastructure share many common goals and challenges. Information sharing must balance a number of equities and be mutually beneficial. The United States must look to its political system to display a high degree of creativity and subtlety in creating a mechanism to share information between government and industry.

Recommendations

Finally, I'd like to offer some preliminary thoughts on how to proceed:

- Make use of an extraordinarily powerful tool we call the **"coalition of the willing"** – a group of organizations and experts that come together to pool their information and their ideas to solve an urgent problem. Such coalitions tend to be formed to share information when common benefits exceed the individual costs, and their inherent flexibility makes them rapidly responsive

to the problems at hand. Such coalitions, however, often need a catalyst and a facilitator. They can also raise anti-trust concerns that could be addressed through legislation.

- Make use of the sector that sits between government and industry. In the parlance of the internet, these are the "dot orgs" such as MITRE, SEI and RAND. Some recent examples of effective dot org actions to support cyber security include:

  - MITRE's initiative in creating and hosting Common Vulnerabilities and Exposures (CVE). CVE is a dictionary that provides common names for vulnerabilities to facilitate collaborative action and to help one enterprise understand what vulnerabilities another enterprise is talking about. This endeavor is managed by an "editorial board" that includes representatives of key security product and operating system vendors, prestigious academic researchers, and members of the national security community. CVE is publicly available on the Web at: cve.mitre.org.

  - MITRE, the Software Engineering Institute of Carnegie Mellon University, and MIT's Lincoln Laboratories are working together for the Air Force on the "Lighthouse" cyber security research program that this Committee initiated. This research will provide, among other things, integrated security solutions for security administrators over a distributed network. Results of this research will be transitioned into operational usage as rapidly as possible, beginning this summer.

  - The initiatives of the SEI CERT (Computer Emergency Response Team) to gather and disseminate information regarding the recent denial of service attacks and to proactively train private sector organizations in establishing teams to handle computer intrusion in the private sector. CERT has established an international forum for the exchange of computer incident response information.

  - RAND's initiative in making use of "day after" seminar exercises with other countries to identify issues in international responses to critical infrastructure attacks and stimulate discussion of remedial action.

  - An initiative MITRE took to convene an Internet Service Provider (ISP) Security Summit of technical experts from internet backbone providers and hardware vendors to identify approaches to be taken to improve internet security against denial of service attacks. The summit, which was held yesterday, was attended by more than 25 participants, and will result in a number of short-term solutions that should be released within a week.

- Create an institute to facilitate the "coalition of the willing" and coordinate cyber security research. The recent National Plan for Information Systems Protection incorporates a suggestion of the President's Council of Advisors on Science and Technology (PCAST) to create an institute to coordinate and fund research on cyber security. We believe, however, that such an institute, to be truly valuable, should not be just a distributor of funds, but should have an organic technical capability that is expert in the cyber security field. Because of the natural synergies between performing and directing research and information sharing, we believe that an institute with a dual charter would be of a great benefit to the nation. The organic technical capability and information sharing focus would be crucial to assuring that appropriate research is funded and that research is effectively transitioned into operational use.

My final and most important conclusion is that there is no single solution to the problem of cyber security and no single organization that holds the key. Providing cyber security will be a continuing challenge and will require extensive collaboration between the public and private sectors. It is clear that the Department of Defense, and the broader national security community, has an important role to play.

This is no small challenge. But the threat is real, and the time has come to move from defining the problem to solving it. MITRE stands ready to help.

Information Assurance
at
MITRE

MITRE has a unique combination of attributes that makes our work in information assurance and the protection of our critical national infrastructure a logical extension of our historical role of operating Federally Funded Research and Development Centers. Since its founding in 1958, MITRE has developed a national reputation in most of the technology areas essential for the information protection mission.

National Security Perspective

MITRE has established strong corporate relationships with many government organizations that will play a vital role in protection of the national infrastructure.

DOD: For more than four decades, MITRE has had in-depth relationships with all of the Military Services, the major Defense Agencies, and the major field commands in information security and information operations programs.

National Intelligence Community: MITRE has extensive relationships with civilian and military intelligence organizations and direct access to threat data vital to the timely interpretation of events/attacks on various elements of the national infrastructure.

FBI: MITRE is currently assisting the National Infrastructure Protection Center (NIPC) housed at the FBI, in their mission to provide warning and analysis of infrastructure cyber attacks as well as supporting their continuing responsibility for investigation of computer crimes and the analysis of open source threat material.

FAA: MITRE operates a Federally Funded Research and Development Center for the Federal Aviation Administration and has essential insights into the safety and information security elements as part of its mission to modernize the air traffic management system.

IRS: MITRE operates a Federally Funded Research and Development Center for the Internal Revenue Service, and plays a key role in assuring the security, integrity, and privacy of electronic filing and of data processing tailored to support better customer service.

Trusted Partner

MITRE, as a not-for-profit private sector corporation, is able to protect the privacy and commercial interests of our national infrastructure providers. We have an established reputation as a trusted agent, performing sensitive product evaluations, alpha and beta testing, system security assessment and proposal evaluations involving proprietary data.

Because MITRE does not compete with, or work for, any manufacturer of information technology or provider of information systems, MITRE can be trusted with proprietary insight into the information security capabilities of an organization's systems and products. At the same time, MITRE can offer organizations an objective understanding and assessment of products and contractor capabilities. This insight and objectivity, coupled with MITRE's information security background, uniquely positions MITRE to provide information security expertise that cannot be found elsewhere.

MITRE has established working relationships as well with other FFRDCs (notably the Software Engineering Institute of Carnegie Mellon University, MIT's Lincoln Laboratory, and the RAND Corporation) and with the academic information security research community

Technical Leadership

MITRE has been a leader in the field of information security since the early 1970s, helping protect the information systems of many government and nonprofit organizations.

MITRE developed the early information security technology and started the evaluation of commercial security products in partnership with the Department of Defense. MITRE is active in all aspects of information systems security, ranging from developing theoretical groundwork, to assisting clients in designing and implementing security solutions for their systems. MITRE specializes in keeping track of the strengths and weaknesses of commercial security technology, and how to integrate it effectively into information systems.

MITRE's expertise in Personal Communications Systems and other wireless communications includes detailed analyses of evolving standards and evaluations of associated security provisions and weaknesses.

MITRE's electronic countermeasures expertise includes jamming, deception and exploitation analyses and prototype development for countering communications, radar, and navigation systems.

MITRE provides engineering support to the Global Positioning Satellite System Program office in designing new waveforms and engineering improvements to GPS vulnerabilities, for both DoD and civilian usage.

MITRE conducts a wide range of simulation and modeling activities, providing simulations of individual sensors through integrated system-of-systems distributed environments. MITRE is modeling Department of Defense dependence on infrastructures, as well as decision making during information attacks.

MITRE conceived, created and hosts the Common Vulnerabilities and Exposures (CVE) web site (cve.mitre.org) that supports both government and industry with a lexicon of all vulnerabilities. Each vulnerability is uniquely identified, described, and given a unique name. For the first time vendors, security experts, and victims can discuss particular vulnerabilities with each other and uniquely identify which vulnerability is under discussion, a great boon to the IA community.

MITRE has a nationwide presence, with headquarters in Bedford, MA; major operating centers in McLean and Reston, VA; Ft. Monmouth, NJ; Colorado Springs, CO; San Antonio, TX; and San Diego, CA; and smaller sites in 41 other CONUS locations (and 15 overseas locations). We apply our information security expertise to our own information infrastructure operating locations and connect them through a secure digital communication network.

Breadth of Experience

MITRE provides information assurance (IA) support to our customers across a variety of technical areas. Our information assurance expertise grew out of our experience in information security, which began in the late 1960s, as well as the work we did in protecting our own electronic resources. It was from our work in designing and implementing filtering routers, firewalls, security assessment software, and intrusion detection software for use on our own systems, that our expertise in this area began. Building on the work we had done for ourselves, MITRE began to support our customers' information assurance needs.

MITRE currently has more than 450 staff working in the IA arena. MITRE's major sponsor is the Department of Defense and the majority of our work in IA is also for the DoD. This support includes policy advice and guidance, product assessments, secure system design and design analysis, research, IA red teaming, cryptography and key management, forensics, secure systems modeling, wireless communication system vulnerability assessment, electronic warfare, and information warfare. MITRE provides support to each of the service and the DoD computer emergency response teams (CERTs), to individual commands and CINCs in designing and implementing secure network operations, to the DoD Computer Forensics Laboratory, and to service and DoD "Red Teams."

MITRE's support to many non-DoD government organizations--including the Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC), the Department of the Treasury, the Department of Energy, and the IRS--involves the

development of secure network operations, the identification and analysis of threat information from open source material, and the analysis of attack methodology.

This breadth of experience across a range of sponsors and technical capabilities has provided MITRE with a broad perspective on the range of threats, countermeasures, and technical and political issues in dealing with information assurance.

MITRE

The MITRE Corporation is an independent, not-for-profit company that provides technical support to the government.

Working in the public interest, MITRE operates as a strategic partner with its sponsoring government agencies. This relationship imposes some constraints on MITRE's business practices, but permits a degree of access and a long-term perspective not available to commercial contractors who compete for government business. Within this relationship, MITRE is able to address complex technical problems of critical importance to its sponsors with a breadth and depth of expertise beyond that available inside the government. A strong information technology base and an integrated systems approach support all of MITRE's work.

The Corporation manages three Federally Funded Research and Development Centers (FFRDCs). These Centers support systems engineering and integration work for Department of Defense (DOD) command, control, communications and intelligence (C^3I), systems research and development work for the Federal Aviation Administration (FAA) and other civil aviation authorities, and systems engineering for the Internal Revenue Service (IRS).

Under the primary sponsorship of the Assistant Secretary of Defense for C^3I, the Air Force and Army are sponsors of the DOD C^3I FFRDC. This Center supports the national security and intelligence community with technical work on command, control, communications, computers, intelligence, surveillance and reconnaissance, by applying its core competencies of "system-of-systems" engineering, systems development and acquisition, process implementation, architectures and interoperability, and technology application. In order to serve as an objective, impartial link between its government sponsors and commercial vendors, the C^3I FFRDC does not compete with profit-making organizations, work for the private sector, or manufacture products.

The Center for Advanced Aviation System Development (CAASD), sponsored by the FAA Administrator, is the FAA's FFRDC. CAASD specializes in the analysis, operations, and technologies of advanced air traffic management systems. CAASD supports its clients with a unique combination of operational knowledge, state-of-the-art understanding of technology, advanced laboratory capabilities, and a top-down view of the entire national airspace system. In order to preserve objectivity and impartiality, CAASD does not manufacture products and works with the private sector only as directed by its sponsor.

Under the IRS FFRDC, MITRE provides strategic, technical and program management advice to the IRS and Treasury Department, focusing on work supporting the modernization of the nation's tax administration system.

MITRE employs approximately 4,500 technical and support staff at its headquarters in Bedford, MA, and Northern Virginia, and at more than 60 sites throughout the world.