National Infrastructure Advisory Council

November 22, 2004

The Honorable George W. Bush
President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC

Dear Mr. President:

We are pleased to submit the final report and recommendations of the National Infrastructure Advisory Council (NIAC) study regarding the Common Vulnerability Scoring System. The NIAC would like to credit and thank Mr. John T. Chambers, President & CEO, Cisco Systems, Inc. and Mr. John W. Thompson, Chairman & CEO, Symantec Corporation for their leadership in this study. The Council would also like to thank the members of the study group and external reviewers for their dedicated efforts.

Bolstering the nation's homeland security is a multifaceted task that requires a wide range of approaches. In addition to assuring the protection of physical infrastructures, cyber security must also be addressed in any security plan. Historically, to address this challenge, large computer security vendors and not-for-profit organizations developed, promoted, and implemented procedures to rank networked information system vulnerabilities. These systems, however, have not exhibited necessary cohesion or interoperability and are limited in scope. The NIAC undertook the Common Vulnerability Scoring System project to propose an open and universal vulnerability scoring system to promote a common understanding of vulnerabilities and their impacts. Security of networked information systems can then be managed most effectively with limited resources by applying them to the most critical vulnerabilities.

The Common Vulnerability Scoring System is a system configured to provide users with a composite score representing the overall severity and risk represented by a vulnerability. With this tool, security professionals, executives, and end-users will have a common language to support vulnerability management.

The Council recommends three different steps for adoption by the Federal government. First, the NIAC recommends the use of the CVSS by all Federal departments and agencies. The NIAC also encourages the Department of Homeland Security (DHS) to promote the CVSS throughout the global vulnerability management community. Additionally, the government should task the National Cyber Security Division and US-CERT to work with the NIAC to find a permanent home for the CVSS to support the user community for updates, tool development, and implementation assistance.

Mr. President, on behalf of our fellow NIAC members, we thank you for the opportunity to serve our country through participation in this Council.

Sincerely,

Erle A. Nye
Chairman of the Board
TXU Corporation
Chairman, NIAC

John T. Chambers
President & CEO
Cisco Systems, Inc.
Vice Chairman, NIAC

Attachments: Summary of Report -- Common Vulnerability Scoring System
Final Report and Recommendation by the Council October 12, 2004.

cc: Vice President Dick Cheney
Frances Fragos Townsend, Special Assistant to the President for Critical Infrastructure Protection, Homeland Security Advisor
The Honorable Thomas Ridge, Secretary of the Department of Homeland Security

QUESTION

Can the Council develop a scoring system to promote the common understanding of vulnerabilities of networked information systems and their impact?

BACKGROUND

In July 2003, the National Infrastructure Advisory Council (NIAC) initiated a research project to promote a common understanding of vulnerabilities and their impact through development of a common vulnerability scoring system. Current scoring systems, in use by the Computer Emergency Response Team/Coordination Center, Symantec, Internet Security Systems, Cisco Systems and others, rate vulnerabilities according to a variety of metrics and determine a single overall threat score by weighing these metrics. These systems use different, non-common metrics to characterize vulnerabilities; they are are focused on the Internet and do not consider other types of networked information systems; they do not universally accommodate changes over time; and they do not have provisions for user operational environments with different risk profiles.

The Working Group developed the CVSS as an open, comprehensive system that addresses these shortcomings and is suitable for international adoption across all types of information systems and environments.

VULNERABILITY DEFINITION AND CLASSIFICATION

To promote a common understanding of the severity of vulnerabilities, a common vulnerability definition must be used. For CVSS, the Study Group used the definition as stated in the NIAC Vulnerability Disclosure Framework report, which was completed January 2004.

A vulnerability is defined as a set of conditions that may lead to an implicit or explicit failure of the confidentiality, integrity, or availability of an information system. Examples of the unauthorized or unexpected effects of a vulnerability may include any of the following:

- Executing commands as another user
- Accessing data in excess of specified or expected permission
- Posing as another user or service within a system
- Causing an abnormal denial of service
- Inadvertently or intentionally destroying data without permission; or
- Exploiting an encryption implementation weakness that significantly reduces the time or computation required to recover the plaintext from an encrypted message

Common causes of vulnerabilities are design flaws in software and hardware, botched administrative processes, lack of awareness and education in information security, technological advancements or improvements to current practices, any of which may result in real threats to mission-critical information systems.

KEY CHARACTERISTICS OF THE CVSS

- The CVSS is designed to provide the end-user with a composite score representing the overall severity and risk a vulnerability represents
  - Using CVSS, security professionals, executives, and end-users will have the basis for a common language with which to support vulnerability management

- CVSS is a modular system with three distinct groups that combine the intrinsic characteristics of a vulnerability
  - Each of these qualities or "metrics" has a specific way of being measured, and each group has a unique formula for combining and weighing each metric
  - CVSS also presents a very simple interface to end-users, because all numeric computation is automatically performed in the background

- The scope of CVSS is constrained to contain only what is necessary to adequately describe information systems vulnerabilities. CVSS does not address any external issues such as:
  - **Potential Threat:** Vulnerabilities that are dependent on the exploitation of other vulnerabilities before they become a risk. For example, consider a vulnerable application that resides behind a firewall, which itself is vulnerable. When scoring the firewall vulnerability, consideration should not be made for the effects of the exploitation of the application or any other secondary vulnerabilities.
  - **Real-time Attack Scoring:** CVSS does not have any capacity for tracking the threats posed by the ongoing exploitation of vulnerabilities. This is a consideration that would be tracked by other scoring systems.
  - **Global Exposure Scoring:** CVSS itself is not a database and has no intrinsic capacity for collating and averaging large amounts of vulnerability scores.

- Vulnerability metrics, in CVSS parlance, are constituent components or characteristics of a vulnerability that can be quantitatively or qualitatively measured These values are clustered together in three groups:
  - **Base**
    Contains all of the qualities that are intrinsic to any given vulnerability that does not change over time or in different environments—a measure of ***severity***
  - **Temporal**
    Contains the characteristics of a vulnerability that are time-dependent and change as the vulnerability ages—a measure of ***urgency***
  - **Environmental**
    Contains the characteristics of vulnerabilities that are tied to implementation and are specific to a user's environment—a measure of ***priority***

The final adjusted score represents the risk a vulnerability represents at a particular point in time for a specific environmental condition

RECOMMENDATIONS

- Support use of the CVSS by all Federal departments and agencies. Those departments and agencies involved in identifying, reporting, and scoring vulnerabilities should develop Base and Temporal scores to contribute to the worldwide body of knowledge for each vulnerability. All departments and agencies should compute Environmental (i.e., Final) scores as they become involved in remediating and resolving vulnerabilities.

- Encourage DHS to promote the use of CVSS by the global vulnerability management community, including international, state, local, and tribal governments, critical infrastructure owners and operators, and discoverers, vendors, coordinators, and users.

- Coordinate with the NIAC to identify an organization to function as the permanent home for CVSS. This organization should be responsible for maintaining and updating CVSS metrics and formulas. It should also possess significant technical expertise and experience managing vulnerabilities, and should maintain a global focus.