THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

VULNERABILITIES TASK FORCE REPORT CHAIN OF CONTROL ISSUES

January 8, 2003

Vulnerabilities Task Force Report

Chain of Control Issues

1.0 Introduction

The Administration has expressed concern that concentration of multiple entities' telecommunications assets in specific locations may have implications for the security and reliability of the telecommunications infrastructure. During the Business and Executive sessions of the National Security Telecommunications Advisory Committee (NSTAC) XXV meeting, concerns focused on telecom hotels, Internet peering points, trusted access to telecommunications facilities, equipment chain of control issues and cable landings.

Following this meeting, the NSTAC's Industry Executive Subcommittee chartered the Vulnerabilities Task Force to examine these issues as well as vulnerabilities in common duct runs, rights of way, and the logical security issues associated with the Open Advanced Intelligent Network (AIN).

The current environment, characterized by the consolidation, concentration, and collocation of telecommunications assets, is the result of regulatory obligations, business imperatives, and technology changes. This construct has created a more diverse network topology but also heightens security concerns. The networks comprising this topology, which are owned and operated by private industry, are the critical infrastructures upon which the Government and other sectors rely. Therefore, security of these networks is of utmost importance.

Each of the aforementioned security issues will be addressed in separate reports. A final executive summary document will be created to highlight each topic and NSTAC recommendations.

2.0 Specific Tasking

The Government has raised concerns with how the telecommunications industry maintains the Chain of Control of the delivery of hardware and software material as it transits from the vendor to the service providers. This report characterizes the situation and the level of control in the industry. This report is based upon discussions with several traditional telecommunication service providers and vendor representatives. This Task Force did not address this issue with respect to Internet Service Providers.

3.0 Discussion of Chain of Control

"Chain of control" is a phrase used frequently in the literature but without specific definition. Such use implies that it is common knowledge or authors are simply using the common dictionary definitions. From the broad context of use in information and network security papers, chain of control refers to procedures or mechanisms put in place to enforce the implementation of security policies without any lapse, whether physical, logical or functional. The complexity and thus the cost in manpower and other resources of the procedures and mechanisms is the result of risk management analysis and decision making, which may range from formal and ultimately made by senior executive authority to informal, implicit and – perhaps – un- or misinformed. Chain of control is not an either/or proposition. It is a spectrum of possible approaches, ranging from complex to non-existent. Complex chain of control mechanisms can include, for example, requiring two or more authorized individuals to supervise or conduct and document each operation or transfer. Simpler mechanisms may rely, for example, on routine precautions (e.g., locked doors or gates), configuration checking (e.g., regression testing) and normal activity documentation (e.g., access logs, shipping documents). Chain of control may also be limited or prescribed by legislative or regulatory requirements for which the affected organization has no reasonable, affordable alternative. Cost, potential losses, past experience and known or suspected threats are the major decision factors in developing appropriate chains of control. In the final analysis, chain of control becomes a business decision. Like all business decisions, it must justify the application of scarce resources in priority over competing needs in – usually – a profit-making environment.

4.0 Hardware Delivery Mechanisms

There is a distinction between how industry manages internal corporate networks and how telecommunications companies manage their commercial public networks. This distinction plays an important part in assessing security implications with respect to public networks.

Industry (as well as Providers in general) purchase equipment destined for their internal corporate networks from a wide set of vendors and usually their Information Technology staff installs the material into their networks. The amount of control these companies maintain varies from tight to very loose. These companies maintain some material, such as desktop computers, in inventory until needed.

Telecommunications providers generally purchase equipment destined for their commercial network from a limited set of trusted vendors. After working closely with the vendor, the provider qualifies each new release of system hardware and software (often in a provider owned test facility) and only then will accept delivery. Historically, telecommunications vendors delivered the material to the customer site, installed, tested, and verified it; then turned it over to the customer. Today several, mostly larger, providers maintain their own cadre of installers. Others rely on trusted installation companies. In any case, companies maintain very close direct or indirect control of the material.

This level of control applies to the switching elements and to the administration, operations, maintenance, and provisioning (AOM&P) systems as well. Despite the level of control exercised by public network service providers and their vendors, the control does not reach the highest level described above in Paragraph 3.0. For this reason, this paragraph discusses the residual risk to compromising the equipment destined for the commercial network.

The complexity of the custom designed equipment and the unique operating conditions (e.g.: complex interconnects, forty-eight volt power, absence of support software programs and databases in the shipped gear, and limited time to act) make the successful modification of the system exceedingly difficult. Further, the specific program loads for each system either are shipped separately from the system, or are re-installed after installation is complete. All of the factors taken together convey the difficulty an adversary would encounter if the adversary undertook the challenge to modify equipment destined for the commercial network. Indeed, the major risk the public network service providers and their vendors face is physical damage to or loss of the equipment. Each shipment is worth a great deal of money and represents a significant investment of time. The economic worth of the equipment drives the protective measures (bonded or vendor owned trucking, air ride suspension trailers, complex way bills, etc.).

5.0 Delivery of Software

Several larger public network service providers test the software and maintain total control of the programs and databases after the vendor delivers the software to the customer. These providers then distribute the software to the various sites in their network. Other public network service providers may use software distribution facilities owned, controlled, and certified by the vendors. In either case, the vendors must demonstrate a careful and controlled software delivery process in order to remain in business.

6.0 Chain of Control Issues

The vendor, or the vendor's surrogate, maintains control of the equipment until the customer accepts it. Upon receipt and after installation, the service provider is responsible for verifying the integrity of what was received and closely controlling the equipment and maintaining the inventory of spare parts and components.

7.0 Conclusions/Findings

The public network service providers and their vendors, in their desire to protect their significant investments, maintain an extensive controlled delivery system for software and hardware components of the public network commensurate with the level of risks discussed above. Consequently, and as significant protection is afforded these custom built and configured systems, the Vulnerabilities Task Force believes that, although security will remain a priority, no policy actions are deemed necessary at this time. However, if networks become reliant on commodity equipment, this could become an issue for consideration.

APPENDIX A – TASK FORCE MEMBERS AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

BellSouth Corporation	Mr. Shawn Cochran, Chair
Electronic Data Systems	Mr. Dale Fincke, Vice-Chair
AT&T Corporation	Mr. Harry Underhill
Bank of America Corporation	Mr. Roger Callahan
The Boeing Company	Mr. Robert Steele
Computer Sciences Corporation	Mr. Guy Copeland
Lucent Technologies	Mr. Karl Rauscher
Nortel Networks	Dr. Jack Edwards
Qwest	Mr. Jon Lofstedt
Raytheon Company	Mr. Robert Tolhurst
Rockwell Collins, Inc.	Mr. Ken Kato
Science Applications International Corporation	Mr. Hank Kluepfel
SBC Communications, Inc.	Ms. Rosemary Leffler
United States Telecom Association	Mr. David Kanupke
Verizon Communications	Mr. Jim Bean
WorldCom, Inc.	Ms. Joan Grewe

OTHER PARTICIPANTS

George Washington University	Dr. Jack Oslund
Lucent Technologies	Mr. Greg Shannon
National Security Council	Mr. Marcus Sachs
Qwest	Mr. Tom Snee
SBC Communications, Inc.	Mr. Paul Hart
SBC Communications, Inc.	Ms. Suzy Henderson
WorldCom, Inc.	Ms. Cristin Flynn