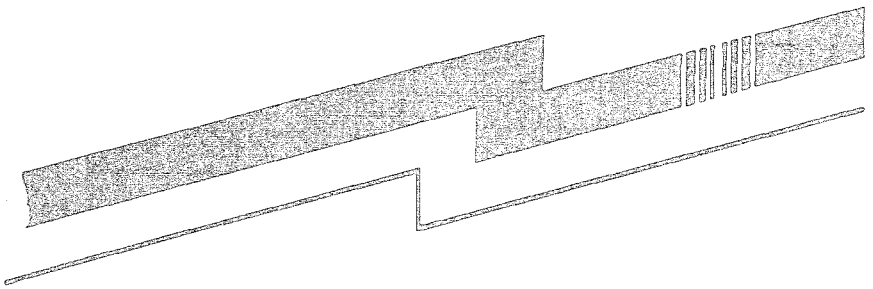

Network Security
Task Force
Report

Report of the Network Security Task Force

November 1990

Report of the Network Security Task Force

November 1990

EXECUTIVE SUMMARY

The Network Security Task Force was established in response to Government concerns about potential disruption of National Security and Emergency Preparedness (NS/EP) telecommunications through network software manipulation.

A significant number of intrusions into the public switched network over the past several years confirm that "hackers" have capabilities to attack the networks and that some networks -- including network elements and operations systems -- are vulnerable to hostile penetration. Service vendors and equipment manufacturers have generally recognized this risk and improvements are underway. Nevertheless, until there is confidence that strong, comprehensive security programs are in place, the industry should assume that *a motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the PSN and monitor or disrupt the telecommunications serving NS/EP users.*

Although the burden of protecting the public switched network falls primarily on service vendors and equipment manufacturers, the task force recommends the National Security Telecommunications Advisory Committee (NSTAC) take the following actions:

1) A follow-on task force should be established that addresses means to reduce the vulnerability of the current public switched network to significant degradations of NS/EP capabilities. The task force should work closely with and in support of the Government Network Security Subgroup. In particular, the task force should:

   - Identify a mechanism and provide an implementation plan for security information exchange concerning risks and remedies

   - Recommend steps to Government agencies that will improve the flow of their intelligence information to industry

   - Recommend to the Government research and development needed for commercially applicable security tools

   - Evaluate existing industry-wide standards activities for network security and make recommendations

   The task force should finish its work in sufficient time for review by the NSTAC at its fourteenth meeting in the summer of 1992.

2) The Funding and Regulatory Working Group should address long-term funding, legal and regulatory issues.

TABLE OF CONTENTS

SECTION 1

INTRODUCTION

1.1 BACKGROUND AND PURPOSE

In early 1990 the Office of the Manager, National Communications System (OMNCS) addressed concerns that were being debated in the national security community about the security of common carrier networks. Aware of the heavy dependence of National Security and Emergency Preparedness (NS/EP) telecommunications on common carriers, the OMNCS moved to clarify, through cooperation between industry and Government, the nature and seriousness of these concerns.

The Industry Executive Subcommittee (IES), at its 21 February 1990 meeting, acted on a Government request to initiate a task force to address the network security concerns. At IES request, the National Security Telecommunications Advisory Committee (NSTAC), at its 29 March 1990 meeting, validated the formation of the Network Security Task Force. The task force has met during a period of seven months in 1990.

The purpose of the current documentation is to report:

- The activities, findings and conclusions of the Network Security Task Force to date, and
- The task force recommendations for follow-on actions.

The IES receives the report in written and oral form at its 7 November 1990 meeting.

1.2 PROBLEM DEFINITION AND SCOPE OF NSTAC ACTION

The IES responded to the Government request in February 1990 by assembling a task force and charging it "to scope the network security issue and to determine whether it is appropriate for NSTAC addressal." The network security issues of concern to members of the Government national security community were collected and coordinated in a meeting of NCS representatives from multiple agencies. A summary of these concerns was presented to the task force at its second meeting, in April.

Following dialogue with OMNCS personnel in early meetings, the industry representatives agreed the scope of concerns the task force would address are as follows:

General Area: Potential threat and vulnerability of the current public switched network and associated operations systems to software manipulation that results in:

- Denial of service to NS/EP users - primary
- Extraction of NS/EP significant information - secondary

Issue: Could a motivated and resourceful adversary, in one concerted event, take down the public switched network

- Solely through manipulation of network software, and
- With predictability?

1.3 APPROACH TAKEN

The first few meetings of the task force highlighted a difference of opinion/perception about the severity of the threat and vulnerabilities. Across the full range of participating companies' statements, initial expressions about the gravity of the situation, i.e. the potential consequences of recent intrusions into network software, varied broadly. Unable to rapidly arrive at consensus on the issue, the task force agreed to take further steps and:

- o Assess and characterize the threat
- o Identify types of manipulation and their likelihood
- o Evaluate potential impact on NS/EP capabilities, and
- o Suggest measures to reduce any vulnerability identified.

With the approval of the IES in May, the task force formed a panel to address potential threats and vulnerabilities. The panel's task was to assess the threats to current public telecommunications networks and the specific vulnerabilities of these networks to network element software manipulation. Composed of subject matter experts from NSTAC member companies, the panel provided outstanding help to analyze and correlate specific evidence and historical events and quantify the threat, to the extent possible.

A series of five panel meetings ensued, extending from May to August. Sensitive information was discussed, with accompanying strong commitment to confidentiality by individual attendees. An oral report by the panel chairman was given to the task force, for its consideration, in August 1990.

Following the report of the panel, the task force explored potential areas of future action that had become evident and measures that might reduce vulnerabilities. In the process of identifying these potential areas for

action, the task force identified actions that were appropriate for industry to undertake by itself and also actions that could be undertaken in coordination with the Government.

1.4 ORGANIZATION OF THE REPORT

Section 2 of this report summarizes the findings and conclusions of the task force. Within section 2:

> Section 2.1 addresses the findings and conclusions of the task force about the threats to the public switched network, its vulnerabilities to the threat addressed, and the resultant risks.
>
> Section 2.2 addresses what the industry members can do on their own to address the vulnerabilities --- in many cases individual industry members have already proceeded with these activities.
>
> Section 2.3 addresses potential actions that could be carried out in the future. Some can be carried out by industry members themselves (e.g. continuing to improve their own networks' security). Certain others could be carried out by industry members together (establishing industry-wide network security standards). Still others (broadening network security information exchange) could be carried out in alternative forms. Some issues are identified that must be addressed, jointly with the Government, in undertaking such a broadening action.

Section 3 contains the recommendations to the NSTAC based on the above task force findings and conclusions.

Appendices A and B list the members of the Network Security Task Force and the Panel on Threats and Vulnerabilities, respectively.

SECTION 2

FINDINGS AND CONCLUSIONS

The task force deliberations have resulted in findings and conclusions in three areas: (1) the threats, vulnerabilities and risks in the area of network software manipulation; (2) industry actions that individual companies can take to reduce current risks of damage; and (3) potential actions that industry, or Government and industry jointly, can take to reduce current risks.

2.1 THREATS, VULNERABILITIES AND RISKS

Regarding the current and recent threat, the task force has reviewed specific information on the evolving capabilities of "hackers" who appear to be targeting the public switched network. In this document, the public switched network includes all public telecommunications service offerings that could affect NS/EP. The term "hackers" refers to computer criminals who intrude into computers illegally or without authorization. These individuals have technical and operational capabilities to penetrate public switched networks. The "hackers" network and share information with each other.

Regarding existing vulnerabilities, the task force has reviewed information on specific penetrations of networks by "hackers" in the past several years. These penetrations have attacked Operational Support Systems and key switching and signalling system elements. In some cases, computer criminals have repeatedly explored some PSN network elements.

The task force concludes:

- There have been software security vulnerabilities in the public switched network and some of these could impact some NS/EP capabilities. Although most security "holes" are "fixed" when discovered, others continue to be identified. Even when fixes are made, not everyone concerned becomes aware of them, and subsequent changes may "undo" the fix. Further, as technology evolves, new security "holes" appear.

- While the PSN is robust with physical redundancy and diversity, there is evidence that there is a new threat to the PSN in the form of computer criminals or intruders who penetrate the various systems of the PSN. The threat to software security is international; penetrations originate in some cases from overseas.

  The individual "hacker" is very capable, even when working on his own. Well-funded adversaries capable of organizing a community of "hackers" will have the capability to launch even more sophisticated attacks. Having the time and resources, such an adversary could build databases and plan and test a widespread attack on the PSN.

- Unless network security is strengthened, a motivated and resourceful adversary could penetrate portions of the public switched network and probably monitor or disrupt telecommunications serving NS/EP users.

The task force reviewed many technical, operational, economic, market and institutional factors that characterize and drive the evolving PSN, and the impact these factors have in creating new vulnerabilities. In a network as complex, heterogenous, and software-driven as the PSN, a high degree of security is technically difficult to achieve. Many features that make the current network excellent with respect to performance, function, and cost make the achievement of high security much more difficult. To over-simplify: open, accessible, customer-driven networks are vulnerable to penetration and software manipulation.

However, the task force also reviewed, in some detail, the steps being taken today to strengthen the network. These involve a mix of technical controls and monitors, personnel practices, operational constraints, and, most important, management commitment. With these measures, security can be significantly strengthened today. In addition, security can be further strengthened by developing a consistent long-term approach, a network security architecture. The task force concludes:

- Strong security in the PSN depends primarily on the actions of individual service vendors and equipment manufacturers that incorporate security features. Security must be wedded to the unique management and administration of each company. Strong security can be achieved with here-and-now measures that have minimal impact on operational costs or network performance.

The task force has been working closely with the Government regarding their perspective of software vulnerabilities of the public switched network. Under the leadership of the Manager of the National Communications System, a Government Network Security Working Group has been established including agencies concerned with telecommunications policy and operation, law enforcement, and national security. It is clear that the Government is very concerned about potential vulnerabilities and attaches a high priority to better understanding this problem in the near future. It recognizes that close cooperation with the NSTAC is essential to meeting its objectives. The task force concludes:

- The Government desires a close working relationship and strong communications among the NSTAC, the NCS, and other Government agencies regarding potential PSN software vulnerabilities and steps to counter them. This relationship should address information exchange, incident reporting and recovery, actions underway in the industry, law enforcement, technical standards, and the potential of Government INFOSEC and COMSEC research and development to focus more closely on PSN security requirements.

Finally, the task force concludes:

- The current risk, which is a function of vulnerabilities and threat, is highly uncertain. Several aspects of the threat are difficult to ascertain: the potential degree of collusion and hostility of "hackers" is not known; the role of foreign "hackers" is undetermined; the support from adversary nations/groups is not quantified; and the deterrent power of law enforcement is just emerging. Consequently, a total threat assessment has not been attempted. In addition, vulnerabilities must be regarded as uncertain: the priority and effectiveness of recent security measures taken by industry are not known; incident risk has been inadequately evaluated; there is a lack of a total system view of security vulnerability; and the capability to respond quickly to an enhanced threat is unclear.

  If the risk is in fact high, it is likely that a body of adversaries could undertake a coordinated attack that would severely degrade the public switched networks' performance capabilities, inducing prolonged nationwide outages. Physical redundancy will not assist in countering this threat.

  If the risk is in fact low, it is much less likely that we will see significant NS/EP service degradation, although the possibility still exists. It is more likely that we would continue to see what we have seen in the past. To date we have not seen the kind of attack that significantly degrades the PSN's NS/EP performance capabilities.

  However, it is imperative that prevailing impressions are eliminated among industry company personnel that "hacker" capabilities are limited to toll fraud. Until there is confidence that strong, comprehensive security programs are in place, the industry should assume that a motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the public switched network and monitor or disrupt the telecommunications serving NS/EP users.

2.2 INDUSTRY ACTIONS TO REDUCE RISKS

The task force identified a number of both near-term and long-term "rational and prudent steps" that individual industry members could take to reduce current vulnerabilities and blunt the existing threat. It should be noted that a number of these steps have been or are being implemented by various companies within the industry.

Eight actions were identified to enhance security in the near-term (Actions A through H). Three further actions (I through K) were identified that will enhance security over the long-term. The actions and steps to achieve them are described in some detail below.

2.2.1 Near-Term Actions

Actions A through H can be undertaken immediately by any individual member company of the telecommunications industry for near-term improvement of its network software security. They represent a prudent approach to enhance the protection of each company's own networks and customers.

Action A: Conduct intensive security evaluations/audits*.

For each company the underpinning for further actions to reduce risk is an initial network software security evaluation/audit, together with continuing follow-on audits. Each company needs to have, internally, the skills to carry out such audits, and to work with vendors on problem areas that come to light. *Most company audits have been carried out with traditional audit groups whose skills and perspectives are different from those required for this kind of audit.* Those conducting these evaluation and audit activities must be capable of looking for intentional wrongdoing, through the application of anomaly detection.

It is clear that companies are unlikely to be in an equal state of network security. Further, companies vary in sophistication in judging their own security. Those regarding themselves as well protected may in fact be more vulnerable than those who are cognizant of a number of problem areas. The task force concludes:

- There is a need for each company to conduct a company-wide intensive and thorough security evaluation/audit. Experience has shown that cursory, or less than complete, security reviews (as described below) may give a company a false sense of network security. The three-level review recommended here is intended to minimize the probability of such an occurrence. A number of the actions subsequently listed will be a direct outgrowth of the findings of such an audit.

---

*The words "evaluation/audit" are used to convey both that: 1) this is intended to be more than a traditional audit; and 2) the rigor and formality of traditional audits are required. The task force noted that traditional audit groups are not likely to have the requisite skills or perspective to conduct these evaluations/audits by themselves. The challenge for each company will be to obtain people with the necessary technical security expertise to participate in conducting these audits. It is expected that each company will need to enlist the aid of appropriate system developers and vendors.

- Company policy review. As with any comprehensive audit, the process should begin by collecting and examining for completeness and adequacy any and all company policies, practices, procedures or other guidelines addressing the security of the company's assets and properties (physical and intellectual). These policies should be reviewed and judged against generally accepted industry standards, and against the practices (to the degree known) of other similar companies. Also, in a more absolute sense, they should be reviewed and judged for adequacy in the face of the known and documented threat to the network and its attendant operations systems from today's computer criminals. Because of the appropriately long lead times and formalities associated with establishing policy in most companies, experience has shown that the official written material regarding network security has not always kept pace with advances in technology or with the changing nature of the external threat. Inadequacies or incompleteness in these areas should be corrected.

While this is a necessary first step in a complete and comprehensive audit, it is by no means a sufficient step. The next two steps must also be completed, if the audit is to be effective.

- Implementation review. Field implementation of the company's policies, practices and procedures should be reviewed next. It is well known that field implementation of a set of policies, procedures and guidelines can differ significantly from the written word. If the prior step has uncovered inadequacies in the company's policies, procedures or practices, this step should still be conducted without delay. It will be valuable to determine just what de facto security practices are in place, and what awareness of security issues and attitudes towards them the field staff has. The results of this step will also be important input to defining or correcting company policies, practices and procedures.

- Site/system review. The final step in the audit process is the most important, the most time-consuming and the most difficult. This step involves detailed audits, including physical site inspections, of security for all of a company's computer-driven assets. In the past, security reviews that have basically stopped with the first two steps have resulted in an overly optimistic view of a company's security posture.

The company will have to take inventory of all of its mechanized, computer-driven systems. Once the inventory is complete, the systems should be categorized roughly as follows. (The audits of systems should proceed through the categories listed in the order given. Those types of systems listed first are the most critical to review.)

1. All systems that are directly involved in the real-time process of completing customers' calls. These are the company's Network Elements. The list of such systems would include all circuit and packet switches, digital cross-connect systems and

real-time network-accessible database systems (such as "Service Control Points" or "Network Control Points").

2. All systems that directly interface with the Network Elements for the express purpose of updating, maintaining or otherwise managing the data elements or programs within the Network Elements. These would include all memory administration systems, service management systems and software generic maintenance systems.

3. All systems that contain sensitive network data or that are involved in critical service-affecting functions. This would include systems that are critical to the establishment of a customer's service (often referred to as "provisioning" systems).

4. All systems that contain sensitive customer data.

Within categories 2 through 4, all Unix® based systems should be reviewed first, followed by VAX/VMS based systems since these operating systems appear to be favored targets of computer criminals.

Each system audit should begin by identifying all vendor or developer provided security features and by explicitly determining which of those features have been purchased or activated by the using company. In addition, all add-on security capabilities should be identified.

Physical site inspections and security reviews should focus on whether or not these security features are being used and how effectively they are being used.

- Site inspections should, for example, determine whether logons and passwords are being shared or not and whether or not they are being properly protected (e.g., not posted on terminals or bulletin boards).

- Particular attention should be given to dial access and access control mechanisms. Password laxity and dial access mechanisms are often the most visible signs of system vulnerabilities.

- Another extremely important area to examine is that of system defaults. Most systems are shipped with startup, or default, accounts, passwords and permissions. It is extremely important to change these default values before the system is put online. A review of the vendor-provided defaults and whether or not they have been changed is a key part of these audits.

- Trash management should be reviewed since trash has been exploited extensively in the past by hackers.

Specific details of this level of security audit will differ for each company and each system. The intent of this step, however, is the

same across companies and systems: to ascertain the actual field implementation of security features and capabilities and to identify any unnecessary vulnerabilities through physical inspection.

Action B: Assure dial access control.

Experience has indicated that very useful and necessary dial access capabilities are a prime point of criminal intrusion into software systems. In fact, one of the very powerful and attractive features of automated, software-driven systems is that they are remotely accessible over the public switched network. Rational and prudent steps can be taken to reduce the probability of this very useful capability being subverted.

- o Eliminate unnecessary ports. All unnecessary dial access ports identified as a result of the audits described above should be eliminated. Previous audits have indicated that old or no longer needed ports are sometimes not deactivated. This step will improve security by reducing the number of possible entry points.

- o Improve dial access procedures. In many instances, improved dial access procedures can improve security. These improved procedures are particularly useful when "occasional" outside (i.e., non-company) personnel must gain access to a system. This can occur when a switch manufacturer, for example, needs access to install a program patch or to test a suspected problem.

  Improved procedures can include manual port activation and automatic de-activation at call completion. Other procedural improvements may also be warranted. These might include restricted dial access permissions and second party access verification. Yet another procedure improvement would be to use "trap and trace" recording procedures on particularly sensitive but hard to control dial access ports. These procedures would create a real-time log of port use.

- o Use security-oriented dial access technologies. Perhaps the most effective action is to undertake the use of security-oriented dial access technologies. While some of these also have vulnerabilities and should not be viewed as panaceas, they can increase overall security. These techniques include:

  - dial-back modems

  - validation of the incoming calling number against an authorization database, and

  - use of dial-in passwords.

  Another available defense is

  - the use of encryption modems at both ends of the dial access connection.

Advanced security capabilities identified in Action E below can also be applied to dial-access ports.

Action C: Use existing security features.

As indicated above, one of the most frequent sources of system vulnerabilities is the simple failure to effectively use existing security features of today's systems. These "use failures" should be identified in the audits discussed above. The task force concludes:

- A variety of employee education and "feature use" action plans can and should be developed and implemented to ensure that existing security features are effectively used on an ongoing basis.

Action D: Require elimination of security "holes".

Most systems seem to have a number of security "loopholes." Either intentionally installed in the system for the convenience of system developers or unintentional software "bugs", these holes create access opportunities for the computer criminal. Well-known but unclosed holes or software bugs in the Unix® operating system were used by Robert Morris in creating and propagating his now infamous "Internet worm".

The intentionally created holes (consisting of undocumented system "defaults", or programmer-created "back-door" entry points into certain subsystems) must be identified and removed by the system developers or vendors. They are virtually impossible for the user organization to discover and eliminate. The unintentional holes (generally software "bugs" or undesirable side-effects of desirable and necessary features) are even harder to find. The task force finds:

- The most effective technique currently known for rooting out these holes is to do a thorough technical "how did they do it" analysis of known system intrusions. This usually requires the expertise of technical security specialists working with knowledgeable systems developers and expert users.

Identifying the holes, while necessary, is obviously not sufficient. The task force concludes:

- Positive action must be taken to expeditiously close all discovered holes, with urgent attention being paid to those that are discovered because they have been exploited by computer criminals. Identified holes can usually most effectively be closed by the system developer. But this means that the existence of the hole must be communicated to the developer and that the user must require that the hole be closed. In the interim, it is incumbent on the using company to devise and apply interim corrective measures.

Action E: Deploy new security technologies

New technologies exist that can significantly improve the security of existing systems. These new technologies can often be appliqued onto the existing systems without major modification to the systems. It is generally felt within the security community that the most effective security mechanisms are those that are carefully architected into a system; however, the security of existing systems can be improved by applique techniques. In fact, some of the newer techniques appear to be particularly adapted to use as a "fence" to "surround" existing systems.

The particular technologies that are most effective and desirable is a topic of much discussion and some disagreement among security experts. However, the following technologies are worth investigating and considering for implementation:

(1) Biometric identity authentication techniques. These include speech verification, hand geometry, retinal blood vessel patterns and fingerprints.

(2) Token-based systems. These generally take the form of small hand-held devices carried by the user that generate a one-time password when activated by a personal identification number (PIN). They also include "smart" cards coupled with authenticators/encryptors located at the originating end of the connection.

(3) Third party authenticators/encryptors. The prototypical system in this case is called Kerberos and was developed at MIT as part of project Athena. In short, the Kerberos approach uses an independent "trusted" (or secure) computer system as a broker between a user and a target system. The Kerberos "broker" knows the password of the user and once it authenticates the user it provides the user with a "token" (an encrypted character string), which will allow the user to access the target system.

These are by no means the only worthwhile technologies to pursue. The task force concludes:

- A variety of new technologies should be explored and deployed as quickly as possible in order to improve existing system security and to enrich the total security environment presenting a variety of defenses to would-be intruders.

Action F: Control proprietary information.

Often computer criminals discover how to break into systems by stealing and reading system and user documentation. The task force concludes:

- Industry members should review their proprietary information protection practices and should institute appropriate and effective controls. All proprietary or sensitive information on paper should be shredded or otherwise disposed of; comparable care should be used in disposing of magnetic media, microfiche, printer ribbons, etc. bearing sensitive information. In no case should sensitive documentation be disposed of by throwing it in the trash bins outside of company offices.

Action G: Improve security staff skills.

Today's computer criminals have sophisticated software skills. Understanding their crimes, their techniques and how to thwart them requires equally sophisticated and knowledgeable security staffs. The task force concludes:

- Industry should evaluate the current skill base of their professional security staffs and take action to supplement that skill base where appropriate. Consideration should be given to emphasizing computer crime prevention skills in security departments along with the more traditional crime prevention skills.

Action H: Establish security awareness programs.

Many companies institute employee security awareness programs from time to time, usually in response to specific incidents. The task force concludes:

- Awareness programs should become a regular and ongoing part of employee information programs. In the final analysis, much of the security of a company's assets will be dependent on awareness and actions of its employees.

2.2.2 Long-Term Actions.

The task force and panel believe that industry members should undertake the following three long-term actions to improve the overall security of their telecommunications networks.

Action I: Develop and implement a network security "architecture".

The task force observed that current telecommunications network vulnerabilities are in part due to the fact that the existing networks have evolved as a collection or conglomeration of individual systems each with its own security architecture. There is, in fact, no consciously designed company network-wide security architecture. In this context, architecture is used to mean concrete, measurable security requirements, and a physical

systems plan for implementing these requirements. Such an architecture would specify the points in a network that require a given type and level of security, and identify feasible implementation alternatives. The task force concludes:

- Industry members with network responsibilities should each develop a total network security architecture and implement it. Such an architecture, in order to be implemented, must be an economically feasible approach targeted at protecting the network from real and quantifiable threats.

In section 2.3, the task force's conclusions are set forth about the need for the industry to develop a consistent set of network security standards. The task force also concludes:

- In developing the company's security architecture and plan, each company should assure that its security architecture is consistent with industry-wide standards as they emerge, and

- The architecture should incorporate effective security technologies that are not overly reliant on user willingness to cooperate or the user's memory. While protection that is sufficient to counter the threat is required, too much of today's security technology is too dependent on onerous user actions.

Action J: Demand, build and purchase secure systems.

Early in the deliberations of the task force, it was noted that suppliers of network elements and systems are motivated primarily by the expressed needs of their customers. The task force concludes:

- If the security of systems is to be improved over the long run, then the acquirers of those systems must demand, build and purchase only systems with appropriate levels of security. This implies that these system "customers" must be able to define their security requirements to their suppliers and must be in a position to objectively analyze the security adequacy of both offered and delivered products.

Action K: Establish effective incident response strategy.

As a result of its investigation of historical incidents, the task force concludes:

- The industry, possibly in coordination with Government, must have a unified and effective plan for responding to software security incidents.

Consistent with such a nationwide response plan,

- Each industry member (service provider and equipment manufacturer alike) must have its own corporate response plan.

These response plans should effectively treat both the immediate response to an incident and the appropriate recovery strategies and tactics. The establishment of such plans is totally consistent with today's NS/EP posture within the industry and in general involves only, one hopes, straightforward extensions to existing plans.

2.3 POTENTIAL GOVERNMENT/INDUSTRY FUTURE ACTIONS

The task force identified a number of actions that could be undertaken in the future either by industry companies themselves without Government sponsorship or by NSTAC in joint action with the Government.

Steps that can be taken by individual industry companies, and in some cases have already been undertaken, have been identified above. The focus of the current section is on potential future actions, e.g., those not yet undertaken. These include actions by individual companies themselves, by individual companies with each other, and/or by companies in coordination with the US Government. The task force concludes:

- The primary actions needed are that individual members of the telecommunications industry take whatever rational and prudent steps are indicated to secure their own networks, to the extent that these steps have not yet been accomplished. An important start would be the actions/steps listed above in Section 2.2.

- The most important potential follow-on action for NSTAC to address is implementing improved exchange of software-related information on threats to, vulnerabilities of, and incidents in the public switched network.

2.3.1 Security Information Exchange (SIE).

The task force addressed the potential advantages of providing a cross-flow of security information among U.S. companies and agencies that have an interest in network software security. Parties to network security information exchanges could include service vendors, equipment manufacturers, and Government agencies (e.g. network users, network supporters, technical experts, law enforcement agencies, and intelligence agencies.)

In order to define objectives, identify issues, and learn about security information exchange from the experience of others, the task force reviewed the following: (1) the current role of the National Coordinating Center and potential extensions; (2) the Bellcore Security Information Exchange Program for its nine sponsors; (3) the activities of the Government Network Security Working Group, including their Threat/Intelligence Subgroup and their Technical Subgroup, a presentation on a concept for a Network Security Focal Point, and the evolving Terms of Reference for the working group; and (4) potential objectives of, actions of, and restraints on public network operating companies regarding security information exchange. It appeared to the task force that value could be added toward the security of the telecommunications industry by providing a security information

exchange not only among local exchange carriers as provided by Bellcore but also among the broader community of U.S. carriers and suppliers, possibly with the Government in a supportive role.

However, the task force identified issue areas that remain to be addressed in order to identify the most appropriate form of network security information exchange. Examples of areas that need further deliberation are listed below:

1) What would be the priority of each of various objectives to be supported by information exchange? Candidate objectives to be prioritized are:

   Reduction of PSN vulnerabilities

   Alerts provided in near-real-time to contain vulnerability and foster recovery

   Increasing visibility to Government and US industry of trends in threats, vulnerabilities, and risks

   Support to law enforcement and increased deterrence to lawbreakers

   Detection of and response to a new threat

2) What kinds of information would, or could, be exchanged? Candidate kinds of information include:

   Security vulnerabilities, including poor operating practices, security "holes"

   Security remedies

   Incidents (Subissues: Which ones would be reported? How quickly? Under what conditions would they be reported? Would anonymity be a requisite?)

   Recovery needs, actions, plans

   Threats, such as provided by law enforcement agencies, network operators, and/or intelligence agencies

3) What would be needed to make security information exchange successful? Candidates include:

   Removal or reduction of legal barriers, real or perceived

   Security and anonymity of information exchanged

   Experienced analytical capability provided at a central exchange point

   Time, and trust among participants

4) Is there a role for Government in a security information exchange program? Candidate roles include information supplier, information user, and observer.

Regarding roles of the Government, the task force finds the following specific sub-issues to be pertinent:

Would the exchange mechanism be involved in determining whether hostile software manipulation was likely to cause specific NS/EP problems?

Would the exchange mechanism be involved in determining whether Government NS/EP user problems being experienced were being caused by hostile software manipulation?

Could the Government play a useful role in detailed vulnerability studies including scenarios, threat modeling, funded support of industry analytical efforts, identification of NS/EP priorities, conduct of national level exercises, etc.?

What Government intelligence and counter-intelligence efforts could be expanded to specifically address public switched network vulnerability to software manipulation?

What could be the role of the NCC in security information exchange?

As a result of the described investigations and deliberations about information exchange, the task force concludes the following:

- Significantly increased exchange, between PSN service vendors and equipment manufacturers, of software related information on threats, vulnerabilities, and remedies could significantly help to reduce vulnerabilities of the public switched network. Initially, emphasis should be placed on measures that will reduce vulnerability rather than provide near-real-time alerts, assist prosecution of computer criminals, or provide trend information.

- Issues remain to be addressed in order to develop a program that would foster the appropriate security information exchange. For example, from industry's point-of-view, what are be the principal objectives of improved security information exchange and what factors would need to be addressed to meet these objectives? In a joint activity between industry and Government, what Government objectives, industry objectives, and mutual objectives should be pursued? Also, prior to establishing such an exchange, clarification of legal and regulatory constraints is needed.

2.3.2 Legal and Regulatory Ramifications to SIE

The task force found that there are a number of legal and regulatory ramifications that must be identified prior to establishing broader coordination or sharing of information about network security incidents.

The impacts of laws and regulations such as the Privacy Act, the Modified Final Judgement, and anti-trust regulation need clarification. In particular, clarification is needed regarding the nature of the information that can be collected and the handling of information that might later become involved in law enforcement actions. Legal experts of potential participants in such an information exchange do not always agree on the ramifications of the above laws and regulations.

Constraints on the sharing of information must be addressed early. Example questions that have been raised and still need to be addressed are:

> Are there any regulatory impediments that restrict telecommunications service providers from exchanging data among themselves regarding intrusion into the network? Might the type or source of the data be key regarding its shareability, i.e. generic break-in information, information about holes in the network, warnings about suspected intrusions or intruders, information that was obtained in the course of business, information obtained through network monitoring activities such as wire-tapping, or information obtained through the monitoring of bulletin boards?
>
> Under what conditions can telecommunications service providers obtain and use information from the network to protect themselves or others from the activities of computer criminals? What evidence is necessary to obtain cease and desist or arrest warrants to stop network intrusions? What evidence is necessary to be able to indict and successfully prosecute network intruders? What constitutes a network intrusion? Must a perpetrator actually do harm to the network or illegally copy, sell or destroy software in order to be successfully prosecuted?
>
> Which federal agencies and departments are responsible for apprehension and prosecution of computer crimes? Governmental responsibility seems to be fragmented. The monetary impact of software losses is difficult to quantify, but law enforcement uses monetary loss thresholds as an artificial barrier before any investigative action is taken. Additionally, local law enforcement officials are generally ill-equipped to deal with the computer crimes. Often when such crimes are proven, penalties are not commensurate with the potential damage that could have been caused. Penalties range from seizure of equipment and files, to probation, to short terms in institutions.
>
> To what extent can law enforcement personnel share information with telecommunications companies? What legal and regulatory constraints are there on the flow of information from local and Federal personnel to private industry telecommunications personnel?
>
> Will the use of information in law enforcement procedures such as grand jury deliberations unduly hamper the dissemination/ coordination/use of such information by industry, even if industry has been the source of the information?

The task force was unable in the time available to address all the legal and regulatory ramifications of common carrier network security information exchange. However, the task force believes:

- The NSTAC's Funding and Regulatory Working Group (FRWG) can work with Government to address the legal and regulatory issues and identify why they are important. Government could work to clarify the situation and NSTAC can review and advise on the clarification.

2.3.3 Industry Criteria and Standards

The development of industry-wide criteria and standards is a potential future action among industry companies. The telecommunications infrastructure comprises hundreds of local exchange and interexchange carriers. Each switching node may be supported by several operations support systems. The protection of network elements and their operations systems, or their secure interconnection, is not covered by accepted industry-wide security standards.

The networks themselves have been designed historically in an environment of trust. Once a craftsperson passes an entrance security check and remotely enters one system, access to another system is typically not blocked. Therefore, if an intruder penetrates defenses at any point of entry, few internal barriers or challenges are raised. Penetration of any "weak link" in the "chain" of network nodes can permit broad access within the network, even from a remote dial-up location.

An adversary can gain access to a system by exploiting a weakness in the security screen or by masquerading as an "authorized" user. Once in the system, he can manipulate system software and network elements.

The trend toward automation is driven by business and economic factors. Further automation of the IEC and LEC interconnection systems (e.g., SS7 signalling systems) is planned. However, in the belief of the task force, two actions can contain the potential damage caused by the present and emerging threat:

1) Insist on installing robust security options on each network element procured by each network provider, and

2) Insist that each employee operate and maintain the security element in a fashion consistent with its intended use.

These two items merely reflect prudent business practices.

Industry-wide security criteria and standards become increasingly important as automated interoperability of networks proliferates. It is not envisioned that the task force would develop new industry standards to address network security shortcomings. The task force should review the current and developing industry standards that support or enhance network security, and determine what network security issues remain. The task force should describe these remaining network security issues in detail and

present them to the appropriate standards organizations for inclusion in their developmental activities.

2.3.4 Research and Development and Technology.

The task force believes that, in future research and development, ways to enhance the network security of the public switched network need to be addressed. Current Government sponsored security research is generally not commercially applicable, is restricted in its use, and is not application-oriented (in particular, intrusion detection research). Coordinated, synergistic work efforts are needed among the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), industry, and possibly academia. Possible approaches to assist in redirecting Government research to commercially applicable security mechanisms are as follows:

- A follow-on task force, involving security research experts, could define problems, provide examples, explore approaches, and provide recommendations.

- A joint industry/Government security research advisory board could provide the industry view to NSA/NIST on an ongoing basis, provide Government research results to industry, and review relevant academic accomplishments.

- Specific action panels with participation from industry and Government could be constituted, for example, to develop a "commercial Orange Book"; intrusion detection devices for carrier networks; and encryption devices that are commercially applicable.

SECTION 3

RECOMMENDATIONS ON FUTURE NSTAC ACTIONS

The task force has concluded that major responsibility for network software security lies with individual service providers. In its report the task force has provided guidance for these service providers that, when followed, will substantially enhance the security of their own networks. Beyond this, it appears that a broader information flow among carriers and suppliers nationwide will assist the carriers/suppliers to improve their network security. Therefore, the task force recommends two follow-on activities:

1) A follow-on task force should be established that addresses means to reduce the vulnerability of the current public switched network and associated operations systems to software manipulation that results in denial of service to NS/EP users, and extraction of NS/EP significant information. The task force should work closely with and in support of the Government Network Security Subgroup that is addressing related issues. In particular,

   - The task force should focus primarily on the identification and development of a mechanism for establishing a security information exchange that will enhance public switched network security. The task force should prepare a detailed implementation plan for establishing a security information exchange. Potential players in such an information exchange could include service vendors, equipment manufacturers, and government agencies.

   - The task force should consider mechanisms that will enable Government agencies to give to industry intelligence information that impacts the security of the network. As part of this process, the task force will define the information that industry needs and how this may be fed into the security information exchange.

   - The follow-on NSTAC task force should examine, in a joint effort with the Government, what network security areas need further research and development relative to the public switched networks, in order to facilitate the development of commercially applicable security tools. As part of this process, the task force should: (1) identify and prioritize needs of the PSN for technical developments; (2) meet with the Government and present an industry view of what is needed to be developed; (3) determine what is already being addressed by the Government; (4) make recommendations on what Government/industry should focus on in the future.

   - The task force should investigate existing industry-wide standards activities for network security, determine if shortfalls exist, and make recommendations as appropriate.

Task force evaluation of the network security issue, coordination of this evaluation with Government representatives, and recommendations to the NSTAC should be completed in sufficient time for review by the Operations Working Group (OWG) and the Industry Executive Subcommittee (IES) prior to the NSTAC's fourteenth meeting in the summer of 1992. As the task force makes progress it should report specific results and recommendations to the OWG, IES, and NSTAC.

2) The Funding and Regulatory Working Group should address long-term funding, legal and regulatory clarifications and potential improvements that could enhance public network software security beyond the level attainable by industry and Government actions in the near term. The FRWG should address section 2.3.2 of this report; the follow-on task force will continue to work in consultation with the FRWG and cite specific areas of concern, particularly with regard to issues that relate to security information exchange.

APPENDIX A

Network Security Task Force Membership

AT&T	Mr. Dave Bush/Mr. Jim Taggart
BELLCORE	Mr. Randy Schulz
CONTEL	Mr. Don Nowakoski
Ford Aerospace	Dr. George Dinolt
GE	Mr. Pat Glenn
GTE	Mr. John Cholewa
ITT	Mr. Joseph Gancie
MCI	Mr. Joseph Cassano
Motorola	Mr. Alexander Toth
NTI	Dr. Jack Edwards
Rockwell	Mr. Larry Manly
UNISYS	Mr. Herb Benington, Chair
UTI	Mr. Jay Nelson

APPENDIX B

Panel on Potential Threats and Vulnerabilities
Membership

AT&T	Mr. Dave Bush/Mr. Jim Taggart
BELLCORE	Mr. Barry Schwartz, Chair
CONTEL	Mr. Doug Guernsey
Ford Aerospace	Dr. George Dinolt
GTE	Mr. Jim Moake
MCI	Mr. Bruce Wells
NTI	Dr. Jack Edwards
UNISYS	Mr. J. Michael Williams
UTI	Mr. John Laclede