

BITS Comments on Level-Oriented Recommendations

LEVEL 1: THE HOME USER AND SMALL BUSINESS

	RECOMMENDATION	COMMENTS
R1-1	Because automated hacking programs scan the Internet for unprotected broadband connections to exploit, those home users and small businesses planning to install a DSL or cable modem should consider installing firewall software first. (Some Internet service providers (ISPs), offer firewall software with DSL or cable modem set up.) Once firewall software is installed, it is important to regularly update it by going to the vendor’s web site.	Supportive. Addresses known attack methodologies and prevents use of personal PCs being utilized as points of attack. Firewalls should be independent of firewall technology type. Recommendation should focus on both hardware and software firewalls.
R1-2	Because new computer viruses are introduced every week, home users and small businesses should regularly ensure that they are running an up-to-date “antivirus system.” (Some antivirus vendors offer automatic updates online. Some Internet service providers scan all incoming e-mail for viruses before the e-mail gets to the user’s computer.)	Supportive. Viruses can plant malicious code on PCs that can be used in subsequent attacks against other machines.
R1-3	Because new viruses often come as e-mail, home users should use caution when opening e-mail from unknown senders, particularly those with attachments. To reduce the number of unknown senders, home users should consider using software that controls unsolicited advertisements, called “spam.” (Some ISPs offer programs to block spam. Some ISPs also offer to block all incoming e-mail except from those friends and associates that the user selects.)	Supportive. Less concerned about this than about the anti-virus and firewall protections. With a good anti-virus package, configured properly, most spam-bred infections would be eradicated. The bigger issue here is around spam attacks that attempt to overload a system into a denial of service. This is more a corporate than a home issue.
R1-4	Home users should also regularly update their personal computer’s operating systems (such as Microsoft Windows, Macintosh, Linux) and major applications (software that browses the Internet or creates documents, charts, tables, etc.) for security enhancements by going to the vendors web sites. (Some software vendors offer automatic updates online.)	Supportive. Most home users do not update their operating systems with the fixes provided to fix known vulnerabilities. This is primarily an awareness problem, but is complicated by the fact that with most operating systems and applications this is not easy to do.
R1-5	Internet service providers, antivirus software companies, and operating system/application software developers should consider joint efforts to make it easier for the home user and small business to obtain security software and updates automatically and in a timely manner, including warning messages to home users about updates and new software patches.	Supportive. This needs to be a collaborative effort. ISPs and anti-virus software companies have been moving in a direction of trying to make the home environment safer. Many offer built-in firewalls and automatic updating. Operating system and application software developers are also trying to fix their software to make it less vulnerable – particularly Microsoft under its “Safe Computing” initiative. The results with these latter vendors is still more talk than show.

BITS Comments on Level-Oriented Recommendations

LEVEL 2: LARGE ENTERPRISES

	RECOMMENDATION	COMMENTS
R2-1	CEOs should consider forming enterprise-wide corporate security councils to integrate cybersecurity, privacy, physical security, and operational considerations.	Supportive. Each of these areas does play a role in cybersecurity and a close relationship between them is warranted. Would suggest that the business continuity function is also a key player and should be involved.

BITS Comments on Level-Oriented Recommendations

	RECOMMENDATION	COMMENTS
R2-2	CEOs should consider regular independent Information Technology (IT) security audits, remediation programs, and reviews of “best practices” implementation.	Guardedly supportive. While of value conceptually, there is a practical question here as well. Many so-called “independent” review firms, including Big 4 firms, often look at these types of engagements more from a future revenue stream perspective (e.g., added consultation work) than from a pure review perspective. The cost to engage these reviews is often quite high for a large enterprise. Independent reviews by qualified firms must add value in order to offset the cost. To develop an appropriate risk mitigation strategy, it is essential that the financial institution be able to identify and understand the controls relied upon by the service provider to mitigate the risks associated with the outsourced application, system or service. For relationships with outsourced providers, security audits or assessments should be required based upon the risk associated with the outsourcing arrangement. And, while each financial institution determines the security requirements for the applications, system or service, the Roundtable and BITS believe that implementation of an industry-wide approach to security-related issues will more effectively provide a common understanding among IT service providers, address known control weaknesses in outsourced IT services, and result in more consistent and appropriate levels of management by financial services companies that outsource IT services. To that end, the Roundtable and BITS Boards of Directors have endorsed the <i>BITS Framework for Managing Technology Risk for Information Technology (IT) Service Provider Relationships and the BITS IT Service Providers Working Group</i> has undertaken a project to develop an Expectations Matrix that would allow service providers to document their practices, processes and controls in the context of the industry and regulators’ requirements.

BITS Comments on Level-Oriented Recommendations

	RECOMMENDATION	COMMENTS
R2-3	Corporate boards should consider forming board committees on IT security and should ensure that the recommendations of the chief information security official in the corporation are regularly reviewed by the CEO.	Guardedly supportive. It may not be necessary to form a separate committee to focus specifically upon cyber security issues. It would seem that an existing board (e.g., Audit Committee) could serve in this role.
R2-4	Corporate IT continuity plans should be regularly reviewed and exercised and should consider site and staff alternatives. Consideration should be given to diversity in IT service providers as a way of mitigating risks.	Supportive. No security plan can be 100% effective. Preparing for those situations in which an organization's security plan is not enough is logical.
R2-5	Corporations should consider active involvement in industry-wide programs to: (a) develop IT security best practices and procurement standards for like companies; (b) share information on IT security through an appropriate information sharing and analysis center (ISAC); (c) raise cybersecurity awareness and public policy issues; and, (d) work with the insurance industry on ways to expand the availability and utilization of insurance for managing cyber risk.	Supportive. Industry-wide programs give all members the opportunity to learn and the opportunity to improve. They also can save time through the sharing of other's best practices.
R2-6	Corporations should consider joining in a public-private partnership to establish an awards program for those in industry making significant contributions to cybersecurity.	Neutral. Not sure of the value of this recommendation as it is not clear who is the target audience of awardees. If vendors, one could argue that they should by mission be making these contributions. If individuals, perhaps there could be merit depending on the selection criteria.
R2-7	(1) Enterprises should review mainframe security software and procedures to ensure that the latest effective technology and procedural measures are being utilized; (2) IT vendors and enterprises employing mainframes should consider developing a partnership to review and update best practices of mainframe IT security and to ensure that there continues to be an adequate trained cadre of mainframe specialists; and (3) IT security audits should include comprehensive evaluations of mainframes.	Supportive. In many industry sectors, including banking and finance, mainframes still play a large role in the processing and housing of information. This recommendation should apply to all systems/platforms not just large mainframe systems. Support of this recommendation should imply that mainframes are less secure than other environments.

BITS Comments on Level-Oriented Recommendations

LEVEL 3: CRITICAL SECTORS THE FEDERAL GOVERNMENT

	RECOMMENDATION	COMMENTS
R3-1	In order to enhance the procurement of more secure IT products, the Federal government, by 4Q FY03, will complete a comprehensive program performance review of the National Information Assurance Program (NIAP), to determine the extent to which NIAP is cost effective and targets a clearly identified security gap; whether it has defined goals to close the gap, whether it is achieving those goals, and the extent to which program improvements, streamlining, or expansion are appropriate and cost effective.	Supportive. Such a review would be supportive of the Federal government leading by example and would help to ferret out if the funding for NIAP has been money well spent.
R3-2	The Federal government, by 3Q FY03, will assess whether private sector security service providers to the Federal government should be certified as meeting certain minimum capabilities.	Supportive. Since many of the Federal government’s service providers also serve the private sector, such certification could be helpful to multiple constituencies.
R3-3	The Federal government, by 3Q FY03, using the E-Government model, will explore the benefits (including reducing resource pressures on small agencies) of greater cross-government acquisition, operation, and maintenance of security tools and services.	Supportive. Not sure the effect of this on security unless this is tied in with the other concepts such as certification. Supportive primarily for the reason that this should result in greater efficiencies.
R3-4	Through the ongoing E-Authentication initiative, the Federal government, by 2Q FY03, will explore the extent to which all departments can employ the same physical and logical access control tools and authentication mechanisms to further promote consistency and inter-operability.	Supportive.
R3-5	Federal departments should continue to expand the use of automated, enterprise-wide security assessment and security policy enforcement tools and actively deploy threat management tools to preempt attacks. By 2Q FY03, the Federal government will determine whether specific actions are necessary (e.g., through the policy or budget processes) to promote the greater use of these tools.	Supportive. Such tools are considered best practices at this point in time and should be fully deployed if not in place already.
R3-6	The Federal government will continue to assess the technical viability and cost effectiveness of various options that provide for the continuity of operations during service outages such as VPNs, “private line” networks and others.	Supportive. This research could lead to spillover to the private sector, which is facing the same questions.

BITS Comments on Level-Oriented Recommendations

	RECOMMENDATION	COMMENTS
R3-7	The Federal government should lead in the adoption of secure network protocols. The Federal government will review new secure network protocols as they are published to determine whether they fill a security gap and whether their adoption would have a cost-effective impact on the operations and security of the Federal government.	Supportive. The Internet’s basic design never included security. Many of the protocols (i.e., the methods it uses in its inter-communication) have flaws from a security perspective. This research will have a positive spillover effect into the private sector.
R3-8	By the end of 2Q FY03, the Federal government will consider the cost effectiveness of a scenario-based security and contingency preparedness exercise for a selected cross-government business process. Should such an exercise take place any security weaknesses shall be included as part of agencies’ GISRA corrective action plans.	Supportive. The scenario development could also be shared with the private sector to assist in business continuity planning and to comply with new requirements outlined in the <i>Draft Interagency White Paper to Strengthen Resilience of the Financial System</i> .
R3-9	OMB, in conjunction with the CIO council, will determine on a case-by-case basis whether to employ a lead agency concept for government-wide security measures. The alternatives will generally include GSA, NIST, the proposed Department of Homeland Security, and the Department of Defense.	Supportive. There are a plethora of agencies involved in cybersecurity at the Federal level – so many so that it is difficult to understand all of their responsibilities and to work with them effectively from a private sector perspective. Having a single agency as a point of contact, or at least having a clearer picture of the primary responsibility of the agencies would be very helpful.

BITS Comments on Level-Oriented Recommendations

LEVEL 3: CRITICAL SECTORS STATE AND LOCAL GOVERNMENTS

	RECOMMENDATION	COMMENTS
R3-10	State and local governments should consider establishing IT security programs for their departments and agencies, including awareness, audits, and standards. State, county, and city associations should consider providing assistance, materials, and model programs.	Supportive. Past the Federal level, the state level support for cybersecurity varies widely from state to state. Some states have good programs, while others typically pay little attention yet all offer the same basic services. At the local level, it is even less robust.
R3-11	State and local governments should consider participating in the established information sharing and analysis centers (ISACs) with similar governments.	Guardedly Supportive. Conceptually, this is a good idea but it comes with many of the same concerns with which ISACs in the private sector come (i.e., protection of shared information).
R3-12	State and local governments should consider expanding training programs in computer crime for law enforcement officials, including judges, prosecutors, and police. The Federal government could assist in coordinating such training and explore whether funding assistance is feasible.	Supportive. When it gets to the law enforcement investigative stage of a cyber incident, state and local law enforcement is often lost. As in the commentary above for R3-10, the abilities vary widely by state and by locality. Ultimately though, most cyber security incidents land up in the legal system and without good knowledge within that system, many potential prosecutions fail to proceed effectively.

LEVEL 3: CRITICAL SECTORS HIGHER EDUCATION

	RECOMMENDATION	COMMENTS
R3-13	Each college and university should consider establishing a point-of-contact, reachable at all times, to Internet service providers (ISPs) and law enforcement officials in the event that the school’s IT systems are discovered to be launching cyber attacks.	Supportive. It is a fact that college and university systems are often exploited to act as points of attack. This recommendation should give that sector the ability to react more quickly to such situations and end attacks more readily.
R3-14	Colleges and universities should consider establishing together: (a) one or more information sharing and analysis centers (ISACs) to deal with cyber attacks and vulnerabilities; (b) model guidelines empowering Chief Information Officers (CIOs) to address cybersecurity; (c) one or more set of best practices for IT security; and, (d) model user awareness programs and materials.	Supportive. All these steps would be effective in shoring up the college and university environment – though again the ISAC concept comes with the cautions previously noted. Also, this is an opportunity to identify the importance of having a comprehensive cyber security education/curriculum for higher education or to establish partnerships/internships between business and education for information security students and professionals.

BITS Comments on Level-Oriented Recommendations

LEVEL 3: CRITICAL SECTORS PRIVATE SECTORS

	RECOMMENDATION	COMMENTS
R3-15	Each sector group should consider establishing an information sharing and analysis center (ISAC) that should cooperate with other ISACs. The Federal government will explore linking the ISACs with appropriate cybersecurity warning-and-analysis centers upon request, and could facilitate the provision of information related to critical infrastructure protection when necessary.	Guardedly Supportive: While information sharing is valuable, the sharing companies must be adequately protected from unintended liability from sharing. In today’s environment, it is not clear if current anti-trust legislation interferes with the sharing of information among competitor institutions. Likewise, there is not adequate assurance that the shared information is adequately protected within the ISACs so as to preclude unintended revelation. Sharing ISAC information with the government could make it publicly available under the Freedom of Information Act to such parties as individuals, competitors, or news agencies. Finally, the current body of law may result in inappropriate liability to the officers and boards of enterprises that share information that does become public. In addition to these concerns, the cost to benefit analysis of belonging to an ISAC must be considered. Most, if not all of the information available from an ISAC is often already available from other sources.
R3-16	Each sector group should consider conducting a technology and R&D gap analysis, in conjunction with OSTP (Office of Science and Technology Policy) efforts to prioritize Federal cybersecurity research to address identified gaps. The sectors and OSTP should coordinate on the conduct of such research.	Supportive. Will require establishment of a lead group by industry (and acceptable to industry participants) to coordinate.
R3-17	Each critical infrastructure sector group should consider developing best practices for cybersecurity and, where appropriate, guidelines for the procurement of secure IT products and services.	Supportive. Will require establishment of a lead group by industry (and acceptable to industry participants) to coordinate.
R3-18	Each sector group should consider working together on sector specific information security awareness campaigns.	Supportive. Will require establishment of a lead group by industry (and acceptable to industry participants) to coordinate.

BITS Comments on Level-Oriented Recommendations

	RECOMMENDATION	COMMENTS
R3-19	Each sector should consider establishing mutual assistance programs for cybersecurity emergencies. The Department of Justice and the Federal Trade Commission should work with the sectors to address any barriers with such cooperation.	Guardedly supportive. Would need to understand better the parameters of the program. Clearly, it is possible to envision a cyber attack involving multiple financial institutions in which a level of cooperation and mutual assistance would have benefit. DOJ and FTC support would be very helpful in understanding and overcoming current legal roadblocks. That said, its important to note that communication and coordination among sectors, intelligence entities, protection agencies, and core service/infrastructure providers is critical in emergency event management.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES SECURING THE MECHANISMS OF THE INTERNET

	RECOMMENDATION	COMMENTS
R4-1	A public-private partnership should refine and accelerate the adoption of improved security for Border Gateway Protocol, Internet Protocol, Domain Name System, and others.	Supportive. These fundamental mechanisms of the Internet were not designed with security in mind. Improvements in them could go a long way toward creating a safer Internet environment.
R4-2	A public-private partnership should perfect and accelerate the adoption of more secure router technology and management, including out-of-band management.	Supportive. Again, the use of routers (i.e., the devices that direct the traffic on the Internet) is a fundamental Internet concept and again one designed without security as a key stimulus. Most large organizations use intrusion detection systems to monitor the router environment, but some do not and likely few small business or home routers are monitored in such a fashion. These present a way in to systems that can then be used to attack others.
R4-3	Internet service providers, beginning with Tier 1 companies or major access providers, should consider adopting a “code of good conduct” governing their cybersecurity practices, including their security-related cooperation with one another.	Supportive. This presents a significant opportunity to proactively monitor/manage attacks and threats at the Internet Service Provider level.
R4-4	A public-private partnership should identify and address fundamental technology needs for the Internet, possibly making use of the existing programs and potentially establishing a fund for such activities.	Guardedly Supportive. Since both sectors are impacted directly by Internet security issues, it does make sense to work together. The reasons for the guardedness are that it will require clear coordination from the private sector and it is not clear how much private sector funding will be needed or how it will be obtained.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES DCS/SCADA

	RECOMMENDATION	COMMENTS
R4-5	A public-private partnership should, as a high priority, develop best practices and new technology to increase security of digital control systems and supervisory control and data acquisition systems (SCADA) in utilities, manufacturing, and other networks.	No comment.
R4-6	Government and industry, working in partnership, should determine the most critical DCS/SCADA-related sites and develop a prioritized plan for short-term cybersecurity improvements in those sites. DCS/SCADA users should consider adopting the Department of Energy’s “21 Steps to Improve Cybersecurity of SCADA Networks.”	No comment.

LEVEL 4: NATIONAL PRIORITIES RESEARCH AND DEVELOPMENT

	RECOMMENDATION	COMMENTS
R4-7	The R&D committee of the President’s Critical Infrastructure Protection Board (PCIPB) should undertake a comprehensive review and gap analysis of existing mechanisms for outreach, identification and coordination of research and development among academia, industry and government. The committee will complete its work and present its recommendations on the need to reform, expand, or establish such mechanisms to the PCIPB in February 2003.	Supportive. Good basic research.
R4-8	The President’s Critical Infrastructure Protection Board should coordinate with the Director of OSTP and the board’s R&D Committee on an annual basis to define a program of Federal government research and development including near-term (1-3 years), mid-term (3-5 years), and later (5 years out and longer) IT security research.	Supportive. Logical fiscal management process.
R4-9	Federally funded near-term IT security research and development for FY04 and beyond should include priority programs identified by OSTP and the R&D Committee. Existing priorities include among others, intrusion detection, Internet infrastructure security (including protocols e.g. BGP, DNS), application security, denial of service, communications security including SCADA system encryption and authentication, high assurance systems, and secure system composition.	Supportive. Federal R&D should have a positive spillover effect to the private sector as the private sector utilizes all of the technologies noted.

BITS Comments on Level-Oriented Recommendations

	RECOMMENDATION	COMMENTS
R4-10	The private sector should consider including in near-term research and development priorities, programs for highly secure and trustworthy operating systems. If such systems are developed and successfully evaluated, the Federal government should accelerate procurement of such systems.	Supportive. The vendors doing operating system development should be conducting research to provide for highly secure and trustworthy software. Their failure to do so in the past is what has led to most of the known vulnerabilities in IT today, and has resulted in significant costs to the private sector by devoting resources to fix vulnerabilities and respond to attacks arising from these vulnerabilities.
R4-11	Federally and privately funded research and development should include programs to examine the security implications of emerging technologies.	Supportive. New technologies that increase productivity are always tempting to potential users. Wireless networking is a good example. It is generally much less costly than wired networks and offers advantages wired networks to not (e.g., ease of portability, quicker built-out). Unfortunately, these types of technologies are still not being designed to incorporate security from their inception. Consequently, not learning from the same lesson we often cite of the Internet, we embrace these technologies for reasons of productivity and cost only to find that they expose our organizations to significant cyber risk.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES SECURING EMERGING SYSTEMS

	RECOMMENDATION	COMMENTS
R4-12	Federal departments and agencies must be especially mindful of security risks when using wireless technologies. Federal agencies should consider installing systems that continuously check for unauthorized connections to their networks. Agencies should carefully review the recent NIST report on the use of wireless technologies and take into account NIST recommendations and findings. In that regard, agency policy and procedures should reflect careful consideration of additional risk reduction measures including the use of strong encryption, bi-directional authentication, shielding standards and other technical security considerations, configuration management, intrusion detection, incident handling, and computer security education and awareness programs.	Supportive. Would suggest this recommendation be enlarged to include not only Federal departments and agencies but private sector companies as well. Any new technology – not just wireless – should be subject to comprehensive security requirements during phases of research and development, design, testing, implementation and support.
R4-13	Government and industry should actively promote awareness for individuals, enterprises, and government of the security issues involved in the adoption of wireless technologies, especially those utilizing the 802.11b standard and related standards. Industry and government should work closely together to promote the continued development of improved standards and protocols for wireless LANs that have built-in, transparent security.	Supportive. Users at all levels need to be made aware of the security risks of emerging technologies – not just wireless.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES VULNERABILITY REMEDIATION

	RECOMMENDATION	COMMENTS
R4-14	A voluntary, industry-led, national effort should consider developing a clearinghouse for promoting more effective software patch implementation. Such an effort may include increased exchange of data about the impact that patches may have on commonly used software systems, including, where practicable, the results of testing.	Supportive. This would be a very helpful process for most companies. Patch management and installation is a time-consuming process and this type of information could help streamline it.
R4-15	The software industry should consider promoting more secure “out-of-the-box” installation and implementation of their products, including increasing: (1) user awareness of the security features in products; (2) ease-of-use for security functions; and, (3) where feasible, promotion of industry guidelines and best practices that support such efforts.	Supportive. (See discussion for recommendation R4-10.)
R4-16	A national public-private effort should promulgate best practices and methodologies that promote integrity, security and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development.	Supportive. This might be a good opportunity to work with CERT on incorporation of these practices into the SEI’s Capability Maturity Model (CMM).

LEVEL 4: NATIONAL PRIORITIES AWARENESS

	RECOMMENDATION	COMMENTS
R4-17	The President’s Critical Infrastructure Protection Board’s Awareness Committee, in cooperation with lead agencies, should foster a public-private partnership to develop and disseminate cybersecurity awareness materials, such as audience-specific tools and resources for annual awareness training.	Supportive. The coordination of the development of this type of material could save private enterprise considerable time and development costs.
R4-18	The StaySafeOnline campaign should be expanded to include national advertising aimed at several audience groups. It should also develop materials for schools and companies.	Supportive. Public announcement spots in the media could be a quick way to raise awareness – especially among the general populace.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES TRAINING AND EDUCATION

	RECOMMENDATION	COMMENTS
R4-19	States should consider creating Cyber Corps scholarship-for-service programs at State universities, to fund the education of undergraduate and graduate students specializing in IT security and willing to repay their grants by working for the States. The existing Cyber Corps scholarship-for-service program should be expanded to additional universities, with both faculty development and scholarship funding. The program should also add a faculty and program development effort for community colleges.	Supportive. Creating a cadre of professionals with requisite cybersecurity defense skills would be a positive step. Finding qualified staff in this area is difficult today, and the increasing focus on security by more companies in the private sector and more government organizations at all levels will only exacerbate this shortage of qualified professionals.
R4-20	The CIO Council and Federal agencies with cybersecurity training expertise should consider establishing a Cyberspace Academy, which would link Federal cybersecurity and computer forensics training programs.	Supportive. Having additional forensics investigation capabilities at the Federal level could help analyze cybersecurity events and provide information important to prevent future attacks.
R4-21	Public and private research labs across the nation should explore the benefits of establishing programs like the Cyber Defenders Program at the Department of Energy’s Sandia National Laboratory.	Supportive. Would assist the research community in focusing greater effort on the defense of cyberspace.
R4-22	The PCIPB’s Committee on Training should explore the potential benefits of establishing a multi-department corps of IT and cyber-security specialists taking maximum advantage of innovative, efficient, and flexible human resource programs. (PCIPB = President’s Critical Infrastructure Protection Board)	Supportive. Improving the cyber security capabilities of the Federal government will offer additional protections in the area of national security, which will extend to the protection of its citizenry and its information. In addition, it should have a cascading effect into the private sector as more is learned at the Federal level and knowledge transfer occurs.
R4-23	State, local and private organizations should consider developing programs and guidelines for primary and secondary school students in cyber ethics, safety, and security.	Neutral. While having some positive effect, it will likely be minimal based on the investment required.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES CERTIFICATION

	RECOMMENDATION	COMMENTS
R4-24	IT security professionals, and IT security associations and organizations, should explore approaches to, and the feasibility of, establishing a rigorous certification program, including a continuing education and retesting program.	Supportive. Security certification/education programs should also be developed and implemented for software developers and system/security administrators. Having a standardized certification program would provide some evidence of a professional’s capability in this area, however, realistically, it is not apparent that comparisons to the medical, legal or accounting professions are accurate. It might also be suggested that others in the IT arena such as software developers and program managers should also evidence some understanding of security issues. If security matters continue to remain the purview of only “security” specialists, the chances of integrating security into all aspects of emerging technology from the ground up will remain weak.

LEVEL 4: NATIONAL PRIORITIES INFORMATION SHARING

	RECOMMENDATION	COMMENTS
R4-25	The Congress and the Executive Branch should work together to remove impediments to information sharing about cybersecurity and infrastructure vulnerabilities between the public and private sectors.	Highly supportive. Current anti-trust laws and the Freedom of Information Act limit information sharing. Likewise, the lack of reasonable protections from civil liability for the officers and board members of “good faith” reporting organizations should be viewed as an impediment.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES CYBERCRIME

	RECOMMENDATION	COMMENTS
R4-26	Appropriate Federal agencies should develop a strategy to encourage citizens and corporations to report incidents of cybercrime, cyber attacks and unauthorized intrusions. In addition, this strategy could also explore mechanisms which facilitate such reporting.	Supportive. See comments for recommendation R4-25.
R4-27	The FBI and Secret Service should continue to improve coordination of their field offices' cybercrime investigations and consider expanding pilot Joint Task Forces.	Supportive. Cooperation between Federal law enforcement agencies should serve to improve investigative and prosecutorial capabilities, which in turn should lead to a lessening of cybercrime.
R4-28	Improve information sharing and investigative coordination within the Federal, State, and local law enforcement community working on critical infrastructure and cyberspace security matters, and with other agencies and the private sector.	Supportive. See comment above to recommendation R4-27.
R4-29	The Federal government should collect survey data regarding victims of cybercrime (i.e., businesses, organizations, and individuals) in order to better establish a baseline understanding of the problem and measure future effectiveness.	Guardedly Supportive. While the motivations behind this recommendation appear noble, absent protections as noted at recommendation R4-25, victims could find their information available for public review and this could create liability issues for the "victim" organizations.
R4-30	The Federal government should review the level of training and funding for Federal, State and local law enforcement for forensic and investigative efforts to address critical infrastructure incidents and cybercrime.	Supportive. Again, better law enforcement responsiveness should serve to improve the investigation and prosecution of cybercrimes, which should in time lead to them diminishing.
R4-31	The Federal government should continue to assess the Federal sentencing guidelines to see if they are adequate for cybercrime.	Supportive. Current sentencing guidelines for white-collar crime in general, the category into which cybercrime often falls, tend to be weak and do not always serve as an adequate deterrent to those considering such crimes.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES MARKET FORCES

	RECOMMENDATION	COMMENTS
R4-32	The President’s Board, working with OMB and in partnership with the private sector and State governments, should review Federal and States regulations and laws that impede market forces from contributing to enhanced cybersecurity.	Supportive.
R4-33	The PCIPB’s Financial and Banking Information Infrastructure Committee (FBIIC), working with the insurance industry, should explore the options for developing an effective risk-transfer mechanism for cybersecurity, including improving risk modeling and availability of loss data.	Guardedly Supportive. On the one hand, the ability to utilize risk transfer mechanisms might suggest to some companies that they need not pay as much direct interest to the subject of cyber security as the overall strategy would suggest they should. On the other hand, if underwriting standards and reviews are strong, this could be helpful in the end to enhance security.
R4-34	Corporations should consider annually disclosing the identity of their IT security audit firm and the general scope of its work, the corporate and board governance system for IT security, company adherence to IT security best practices or standards, and corporate participation in ISACs and other IT security programs.	Neutral. While conceptually similar to the reporting requirements that existed during the Y2K remediation period, absent a clearer understanding of the proposed standards it is difficult to either give support or to offer opposition to this recommendation. It is a bit concerning that the standards suggest very specific areas of disclosure that may or not may be appropriate or cost-justified for all firms.
R4-35	The President’s Critical Infrastructure Protection Board, working with the Institute of Internal Auditors and Corporate Board Members Association and similar groups should continue and enhance the effectiveness of programs of awareness and best practices.	Supportive.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES PRIVACY AND CIVIL LIBERTIES

	RECOMMENDATION	COMMENTS
R4-36	The Executive Branch should consult regularly with privacy advocates, industry representatives and other interested organizations to facilitate consideration of privacy and civil liberties concerns in the implementation of the National Strategy, and to achieve solutions that protect privacy while enhancing network and host security.	Supportive. Protection of fundamental civil liberties should be a goal of this program, as it is with the overall Homeland Defense effort.
R4-37	As part of the annual departmental IT security audits, agencies should include a review of IT related privacy regulation compliance.	Neutral. This appears a reasonable recommendation, however, it is not completely clear what the costs and resource needs of such a program would involve.
R4-38	The appropriate Federal agencies should conduct reviews of the IT security issues related to the implementation of the Gramm, Leach, Bliley Financial Modernization Act and the Health Insurance Portability and Accountability Act.	Supportive. This would seem to already be in place at least for GLBA.

LEVEL 4: NATIONAL PRIORITIES CYBERSPACE ANALYSIS AND WARNING

	RECOMMENDATION	COMMENTS
R4-39	ISPs, hardware and software vendors, IT security-related companies, computer emergency response teams, and the ISACs, together, should consider establishing a Cyberspace Network Operations Center (Cyberspace NOC), physical or virtual, to share information and ensure coordination to support the health and reliability of Internet operations in the United States. Although it would not be a government entity and would be managed by a private board, the Federal government should explore the ways in which it could cooperate with the Cyberspace NOC.	Guardedly Supportive. While this effort would clearly facilitate the sharing of cybersecurity information across a broader spectrum of constituencies and probably positively affect the speed of information exchange, we remain concerned about the protection of that information and the issues noted at recommendation R4-25.
R4-40	The Federal government should complete the installation of the Cyber Warning Information Network (CWIN) to key government and non-government cybersecurity-related network operation centers, to disseminate analysis and warning information and perform crisis coordination.	Supportive. This would be a very positive step in focusing the Federal government's analysis and notification capabilities.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES CONTINUITY OF OPERATIONS, RECOVERY, AND RECONSTITUTION

	RECOMMENDATION	COMMENTS
R4-41	Industry, in voluntary partnership with the Federal government, should complete and regularly update cybersecurity crisis contingency plans, including a recovery plan for Internet functions.	Guardedly supportive. We would support the development of cybersecurity contingency plans, but would like assurance that the Federal government’s involvement would be as a partnership and not as a subtle way of regulatory oversight.
R4-42	The Federal government should review emergency authorities and determine if the existing authorities are sufficient to support Internet recovery.	Supportive. It would seem a good step and a logical step to understand existing authorities before the nation encounters a major cyber attack.

LEVEL 4: NATIONAL PRIORITIES NATIONAL SECURITY

	RECOMMENDATION	COMMENTS
R4-43	The United States should establish a vigorous program to counter cyber-based intelligence collection against U.S. government, industry, and university sites.	Supportive. This seems a logical protection though it is a bit disconcerting to recognize this is a recommendation and not an existing capability.
R4-44	The National Security Council should lead a study to improve understanding of incident response coordination for significant cyber attacks among law enforcement agencies, national security agencies, and defense agencies.	Supportive. This should serve to strengthen the ability of the law enforcement and security communities to respond to a cyber attack.
R4-45	The United States should continue to improve its ability to quickly attribute the source of threatening attacks or actions, seeking to develop the capability to suppress threats before attacks occur.	Supportive. This seems a logical capability to possess.
R4-46	The United States should continue to reserve the right to respond in an appropriate manner when its vital interests are threatened by nation-states or terrorist groups engaged in cyber attacks.	Supportive. This seems a logical capability to possess.

BITS Comments on Level-Oriented Recommendations

LEVEL 4: NATIONAL PRIORITIES INTERDEPENDENCIES AND PHYSICAL SECURITY

	RECOMMENDATION	COMMENTS
R4-47	Public-private partnerships should identify cross-sectoral interdependencies both cyber and physical. They should develop plans to reduce related vulnerabilities, in conjunction with programs proposed in the <i>National Strategy for Homeland Security</i> . The National Infrastructure Simulation and Analysis Center should support these efforts.	Highly Supportive. It is apparent today that cross-sector interdependencies exist; yet there is no way to address them effectively. See comment on cover letter under “Address Critical Interdependencies.”
R4-48	Owners and operators of information system networks and network data centers should consider developing remediation and contingency plans to reduce the consequences of large-scale physical damage to facilities supporting such networks. Where requested, the Federal government could help coordinate such efforts and provide technical assistance.	Supportive. This seems a logical and appropriate action.
R4-49	Owners and operators of information system networks should, possibly working with the Federal government on a voluntary basis, develop appropriate procedures for limiting access to critical facilities.	Supportive. This seems a logical and appropriate action.

LEVEL 5: GLOBAL

	RECOMMENDATION	COMMENTS
R5-1	The Federal government, in coordination with the private sector, should work with individual nations and with nongovernmental and international organizations to foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge. In addition, such networks could help support efforts to investigate and respond to those attacks.	Supportive. Many attacks begin in other nations and spread across the globe. This capability should provide the ability to receive forewarning of events beginning in other countries.
R5-2	The United States should encourage nations to accede to the Council of Europe (COE) Convention on Cybercrime or to ensure that their laws and procedures are at least as comprehensive.	Supportive. This seems an appropriate step that should encourage global law enforcement.
R5-3	The United States should work together with Canada and Mexico to identify and implement best practices for securing the many shared critical North American information infrastructures.	Neutral. While sounding conceptually reasonable, the reality would seem that such a limit is artificial when one considers the global nature of the cyber infrastructure and this would seem as well to be a subset of other recommendations more global in their nature.

BITS Comments on Level-Oriented Recommendations

	RECOMMENDATION	COMMENTS
R5-4	The United States should work through international organizations and in partnership with industry to facilitate dialogue and partnership between foreign public and private sectors on information infrastructure protection, and to promote a global “culture of security.”	Supportive. This seems an appropriate step toward fostering global cooperation.
R5-5	Each country should be urged to appoint a national cyberspace coordinator.	Supportive. This seems an appropriate step toward fostering global cooperation and information exchange.
R5-6	The United States should draw upon the global science and technology base by pursuing collaborative research and development in cybersecurity.	Supportive. Bringing multiple, global resources to bear in the R&D arena should result in better, and perhaps quicker, research results.

BITS Comments on Level-Oriented Discussion Items

LEVEL 1: THE HOME USER AND SMALL BUSINESS

	DISCUSSION ITEM	COMMENTS
D1-1	The biggest business in America is small business. Working through the SBA, many small businesses are able to obtain loans guaranteed by the Federal government. Increasingly, the cybersecurity of small business can impact its employees and the broader economy. Should SBA loans require an IT security checklist?	In making any loan, the lender must consider those risks that could preclude the borrower from repaying the debt. Certainly, in today’s world, the risks presented by cyber incidents have grown significantly – so much so that they have probably become a legitimate risk for a lender to consider in its loan analysis.
D1-2	How can parents and children create a useful dialogue about securing their families’ cyber-space? Cybersecurity is an area where parents and children each bring their own experience and expertise. By sharing these experiences, families can improve the cybersecurity of their household and contribute to an overall increase in America’s cybersecurity.	It is a reality that often the children in today’s families know more than their parents about how to use cyberspace. That would suggest that part of the answer to this question lies in better education aimed at the parents regarding both the risks and protections that are available. Likewise, part of the answer lies in educating our children better about the risks they face while in cyberspace and how to protect themselves. As an example, we teach our children how to deal with strangers when they encounter them in the physical world. We should extend that same teaching to how to deal with them in the cyber world.

BITS Comments on Level-Oriented Discussion Items

LEVEL 2: LARGE ENTERPRISES

	DISCUSSION ITEM	COMMENTS
D2-1	Cybersecurity is a constant process, which requires regular assessments and remediation. Accordingly, cybersecurity can be enhanced with regular IT security audits. How often should large enterprises have cybersecurity audits performed by outside auditors?	It is important to recognize that outside auditors are involved today in reviewing most major companies' cybersecurity. In most firms, the outside auditors already consider cyber security as a part of their annual financial statement certification process. In addition, many firms today contract to have SAS70 reports completed by outside auditors and most of these cover some aspect of cybersecurity. Before deciding on the frequency of such reviews, we first need to spend more time discussing the ultimate purpose of these reviews. For example, is it to inform a company's management of improvements it can make in its cybersecurity environment? Is it to provide a vehicle for public reporting of a given firm's cybersecurity?
D2-2	Cybersecurity is an integral component of a company's operations. When a company makes cybersecurity a management issue, it can better protect its intellectual property and its business operations. What should financial analysts and investors ask companies about their security programs before investing?	A company should be prepared to answer fundamental questions about its security policies and practices in a number of areas including how it protects its networks and its perimeter from attack, how it authorizes users to obtain information, what types of internal risk analyses it uses to monitor and improve its own security and how it protects its customers and its own information. These are the kinds of questions we ask of our business partners.
D2-3	How can large enterprises facilitate the identification and implementation of best practices for cybersecurity?	This is best done through cooperative participation with peers both within the financial services industry and information security experts.
D2-4	Should the National Security Telecommunications Advisory Committee and the National Infrastructure Assurance Council examine the need and possible benefits of establishing an independent organization, similar to the accounting profession, which would develop standards, guidance, and auditing procedures for IT security enterprises?	Further discussion of this idea is worthwhile.

BITS Comments on Level-Oriented Discussion Items

LEVEL 3: CRITICAL SECTORS THE FEDERAL GOVERNMENT

	DISCUSSION ITEM	COMMENTS
D3-1	Should Federal agencies be required to comply with a maximum time limit for the implementation of patches for known vulnerabilities?	This appears to be an emerging best practice in the private sector, and one that should be considered seriously within the government sector. Fixing vulnerabilities is a complex process involving multiple, and sometimes manual, efforts. It is not always easy to dictate fixed time parameters, but certainly it is appropriate to fix the level of attention and response to various levels of vulnerabilities.
D3-2	Should the CIAO or CISO be different than the CIO?	No comment.
D3-3	How should civilian agencies expand use of PKIs for specific situations?	PKI is one of the methods that can be used for user authentication and authorization as well as for validating the source of information. This methodology should not necessarily be studied on a stand-alone basis, but as part of a larger discussion of best practices around tools and techniques and the appropriateness of their application in various situations.

BITS Comments on Level-Oriented Discussion Items

LEVEL 3: CRITICAL SECTORS STATE AND LOCAL GOVERNMENTS

	DISCUSSION ITEM	COMMENTS
D3-4	How can Federal, State, and local governments enhance coordination and crisis management for cybersecurity?	It would seem logical that a government-oriented Information Sharing and Analysis Center covering all levels of government would be a first step in this process. It would also seem logical to establish various forums in which representatives of the various level of government could meet and discuss/share their security concerns and solutions.
D3-5	What special legal or policy challenges might States face in developing an interstate ISAC?	No comment. Leave to others (e.g., states’ attorneys general) to respond.

LEVEL 3: CRITICAL SECTORS HIGHER EDUCATION

	DISCUSSION ITEM	COMMENTS
D3-6	What are the merits of adopting a model set of authorities for IHE CIOs, the academic institution, and the nation? (An example of such authorization can be found at http://www.indiana.edu/ .)	This would seem an appropriate direction in which to move. Given the level of computing power present in IHEs, the current relative openness of access to this availability, and the fact that IHEs are historic sites used to launch attacks, a set of common principles around authorization would be helpful.
D3-7	Should consideration be given to tying State or Federal funding to IHEs to compliance with certain cybersecurity benchmarks?	This would seem to be a good incentive to assure that cybersecurity would receive serious attention from the IHEs.
D3-8	Should an ISAC for the higher education community be established? If so, how? What other steps could be taken to improve methods of information sharing among IHEs at all levels?	An ISAC would be a helpful step in the sharing of vulnerability and attack information. Like other ISACs, the IHE community would logically establish it with assistance from the various government agencies that assist all the existing ISACs. As to other methods, the sector could work within existing professional affiliations (as the FI industry does through BITS) to establish sharing forums.
D3-9	Should IHEs adopt the NIST Information Technology Security Assessment Framework (“NIST 3”) as a standard for information system security compliance?	There are a many standards including NIST’s and others (e.g., ISO17799) that one can use to gauge the adequacy of an organization’s information security processes. There are three key points around this item. First, all organizations should be encouraged to assess with consistency their information security. Second, it seems inconsistent to suggest adopting this type of standard for one sector and not others. Third, consistent with the theme of the overall Strategy, organizations should be encouraged but not required to adopt any single standard.

BITS Comments on Level-Oriented Discussion Items

LEVEL 3: CRITICAL SECTORS PRIVATE SECTORS

	DISCUSSION ITEM	COMMENTS
	No discussion items noted in Strategy draft.	

BITS Comments on Level-Oriented Discussion Items

LEVEL 4: NATIONAL PRIORITIES

	DISCUSSION ITEM	COMMENTS
D4-1	How can government, industry, and academia address issues important and beneficial to owners and operators of cyberspace but for which no one group has adequate incentive to act?	There would seem to be a few methods that can be employed. First, the creation of consortiums among the noted sectors can and should be created in order to share information and create common direction. Second, since the point specifically addresses owners and operators of cyberspace, the use of incentives such as tax credits to these parties for measurable improvements might be considered to enhance incentives. As a last resort, requirements in the way of regulations might be an option.
D4-2	How could out-of-band management for routers be implemented on the Internet, and what are the costs and benefits?	No comment.
D4-3	How should private sectors craft outreach programs to reach all levels of the DCS/SCADA user community to increase awareness of vulnerabilities, consequences, and mitigation measures?	No comment.
D4-4	What training courses and materials should such programs include to equip DCS/SCADA users with the skills necessary to improve security?	No comment.
D4-5	Technology transfer, the process by which existing knowledge, facilities or capabilities developed under Federal R&D funding are utilized to fulfill public and private needs, must be enhanced. The most vital part of technology transfer, the adoption of new security technologies by the private sector, especially the vendor communities, should be the object of discussion for a private / public partnership. What mechanisms could effectively be applied to encourage the adoption of existing and emerging security technologies by vendors?	First, if one assumes that Federal R&D funding typically comes from public tax revenues, it should not be automatically assumed that technologies developed with that funding should go to the vendor community. In essence, that means that corporations and individuals whose taxes funded the research pay twice for the technology – once via their taxes and again by having to purchase the technology from a vendor. Consideration should be given to how this technology can be transferred directly to the user community.

BITS Comments on Level-Oriented Discussion Items

	DISCUSSION ITEM	COMMENTS
D4-6	What are the potential security and privacy implications of emerging technologies such as wireless LANS?	Emerging technologies offer potential enhancements to the way we do business, but we must be very careful that the technology does not advance so rapidly that we lose sight of its security implications. That would be analogous to inventing a car that travels at a very high rate of speed with great gas mileage, but whose design lacks brakes, seat belts, and other safety features. The specific example used in the discussion point of wireless LANs is a good one. Wireless LANs do indeed have many advantages. They are simple and inexpensive to install when compared to wired LANs, they have almost the same capabilities of a wired LAN, and they are relatively inexpensive to purchase. The unfortunate downside – it is rather easy for anyone with a PC that has an antenna and easily available software to intercept what is moving across the LAN including confidential emails and customer data. Vendors, driven by profit motive, attempt to push this technology by stressing the advantages and downplaying the security issues. The security implications are that organizations are installing these technologies without worrying about their security, and in turn opening themselves – and potentially others who use them to exploit others – to data theft, hacking and other malicious activities.
D4-7	Should government work closely with emerging technology product vendors to promote disclosure of the vulnerabilities associated with their products’ use and encourage vendors to make security easier to apply for the average user?	Yes. As well, government refusal to purchase insecure technologies would be helpful.
D4-8	How and by what means should curriculum for software engineers change to reflect more secure coding practices?	Colleges and universities should require software engineering majors to take courses that deal with designing security into their software. Most IHEs do not require this type of coursework in their current curriculum. The curriculum should include a variety of subjects including those software techniques that prevent and facilitate vulnerable software, as well as material around other key security concepts such as authentication and authorization techniques. In addition, the curriculum should address the costs to society and to organizations of poor security.

BITS Comments on Level-Oriented Discussion Items

	DISCUSSION ITEM	COMMENTS
D4-9	Is there an appropriate way to define standard time limits for the patching of systems?	This time required to patch systems varies based on a number of factors such as size of the IT environment, complexity of the environment, and disparity of the environment, that it is extremely difficult to set specific time parameters.
D4-10	What metrics should be used to measure cybersecurity awareness for various audiences and the effectiveness of cybersecurity warnings?	Metrics could include such items as vulnerability alerts distributed, speed of remediation by criticality of vulnerability, and completeness of vulnerability patching.
D4-11	What roles can private citizens play in raising awareness about cybersecurity?	The typical citizen would have a difficult time determining the existence of software vulnerabilities. At most, it would seem they could keep themselves aware of the existence of vulnerabilities and maintain their own equipment and software to keep it secure. As suggested in the Level addressing home users, however, many still require education to understand the risks of vulnerable software as well as finding sources of information that describe the vulnerabilities.
D4-12	How can government and private industry establish programs to identify early students with a demonstrated interest in and/or talent for IT security work, encourage and develop their interest and skills, and direct them into the workforce?	Identification of students would probably not be easy. Computer science and business systems instructors could be used to attempt to identify such students, as could a process of self-selection by the students themselves. The ideas mentioned in the recommendations regarding scholarships for such students and the creation of a Cyber Corps could be helpful in encouraging those students to pursue a security career.
D4-13	How can government and industry identify national training and education standards for cybersecurity professions that will meet the demands of U.S. enterprises?	They could work with various constituencies such as industry forums focused on security (e.g., BITS), current testing organizations recognized to have the best current programs, organizations that develop testing for other professions and highly regarding professional security organizations to determine the criteria for training and testing.
D4-14	Should an accrediting body be created that would set a baseline standard for system administrator-level security knowledge requirements?	Not necessarily. While security is important, and systems administrators should be well aware of how to maintain security within the environments they administer, it is not clear that a formal accreditation is necessary.

BITS Comments on Level-Oriented Discussion Items

	DISCUSSION ITEM	COMMENTS
D4-15	Should other levels of the IT security profession be considered for peer certification or accreditation?	There is a stronger argument for IT professionals whose primary job function is IT security. One note of caution would be to recognize that testing would have to be introduced over an extended period. If immediate certification becomes a requirement, most current professionals would not meet the certification criteria and the profession could lose many good people with a resultant shortage in qualified professionals.
D4-16	Should the Federal government provide support to ISACs such as funding, technical tools or facilities?	Yes, such funding would facilitate the operations of the ISACs. Such funding, however, should not come with an associated concept that it permits the Federal government automatic access to the information held by the ISAC. Such access could inhibit participation by sector participants fearful that information they report could become public knowledge.
D4-17	How may victims rights groups aid in creating greater awareness about the potential dangers of cybercrime?	Certainly, victims rights groups can lobby for greater awareness as they do for all areas of crime for which they exist. They could also assist in enhancing the justice systems understanding of the effects of cybercrime, which could lead to tougher sentencing guidelines for offenders. Victims of cybercrime may not be eager to come forward publicly. Corporate victims in particular would probably remain averse to publicly advocating at the risk of their customers realizing a breach had occurred.
D4-18	Is there a gap between Federal, State, and local laws on cyber-crime? If so, what are the implications	One could argue that the gap is similar to the gap that exists around most white-collar crime situations. Frequently, different levels of government have different prosecutorial and sentencing guidelines around such crimes. Because the level of prosecution is often tied to the level of loss in such crimes (i.e., bigger loss situations tend to be handled at the Federal level while smaller ones tend to go to the state or local level), the gaps result in inconsistent prosecution and sentencing results.
D4-19	What lessons can be learned from the “Basel Capital Accord” that might drive cybersecurity improvements in other infrastructures?	The new Basel Capital Accord proposes amendments to regulation of large banking institutions in the area of operational risk. Banks will need to place an even greater concentration on risk management and mitigation of operational risks, including technology related and cyber risks. BITS has a working group devoted to this aspect of operational risk. Basel, however, only applies to financial institutions. The concept of risk management can be applied to other industries as well.

BITS Comments on Level-Oriented Discussion Items

	DISCUSSION ITEM	COMMENTS
D4-20	Should there be a review of State and Federal requirements for disclosure of information which could help potential attackers; e.g., State filings?	Yes. Organizations are required to file a great deal of information with various levels of government, much of which tends to offer insight into the organization’s internal operations. Unless such information is protected effectively, it could be exposed to individuals with less than honorable intentions who might exploit it against a given organization.
D4-21	How can industry be encouraged to incorporate appropriate privacy protections into their planning and products, using flexible, non-regulatory approaches?	Increasing customer demand is already causing this to happen. Our industry has historically handled information that is clearly important to our customers that we keep confidential as it involves their financial situation. Therefore, we have always had a focus on protecting such information. Within our industry, keeping such information confidential is now also often required by regulation (e.g., GLBA). This trend is moving into other industries (e.g., HIPPA for health care). In all these cases, one can trace the roots of these regulations for increasing public demand for privacy of their information. This demand is likely to increase as more people realize the vulnerabilities that can exist in computer systems and as more media coverage focuses on breaches in security.
D4-22	How can government organizations work to facilitate harmonious approaches in privacy across jurisdictional boundaries?	Where regulation is deemed necessary, having it occur at the Federal level with less of an option for its modification at the state or local level is helpful. This is especially true for national companies.
D4-23	How can the Federal government and the private sector develop people with the ability to “deep dive” data and detect patterns of attack?	The primary ways to achieve this are through a willingness to invest in people who are focused on forensic work and by a constant investment in their training.
D4-24	It took over four decades to develop an indications and warning capability for conventional and nuclear threats. How can the United States develop a similar “incidents and warning” architecture to protect against cyber threats that would be highly effective?	It would seem this could best be developed by a focused consortium effort of the public, private and academic sectors.
D4-25	Is there a need for a new authority, which is not anchored in war mobilization and national defense, to manage priority delivery of goods and services for critical infrastructure purposes?	It would seem existing regulatory authorities already have this mandate and that no new authority is needed.

BITS Comments on Level-Oriented Discussion Items

	DISCUSSION ITEM	COMMENTS
D4-26	Identifying the key infrastructure interdependencies requires an active discussion between the public and private sectors. What processes should be established to help shape how the Federal government prioritizes and funds interdependency and vulnerability studies?	Existing agencies that regulate various industry sectors should work with those sectors to identify such interdependencies. In addition, a broader effort is probably needed across sectors to identify inter-sector dependencies. An approach similar to that taken during the Y2K-remediation period could be used to facilitate this latter effort.
D4-27	Because cyber attacks can be launched from anywhere in the world, it is important to develop capabilities to rapidly determine the origin of an attack or exploit in order to respond effectively. This capability, commonly referred to as “attribution,” is central to determining if an attack is sponsored by a foreign power. How can government and industry analysts enhance attribution capabilities in order to more rapidly identify the source of an attack?	There should likely be a centralized repository for the sector ISACs to feed information. This must, however, be structured in a way that assures the confidentiality of any reporting organization’s information.
D4-28	How can the national security community enhance the discipline of counter intelligence analysis to better support cyberspace security?	There are a myriad of Federal agencies with responsibility for cybersecurity. A first step might be to restructure these responsibilities into a cohesive agency or group of agencies with specific and clear responsibilities.

BITS Comments on Level-Oriented Discussion Items

LEVEL 5: GLOBAL

	DISCUSSION ITEM	COMMENTS
D5-1	What role should the private sector play to best assist developing countries in establishing a “culture of security?”	The private sector contains many organizations whose scope reaches across the borders of the U.S. One of the roles the private sector can play relates to each organization’s internal programs around cybersecurity. If organizations emphasize cybersecurity to their employees, educate their employees about its importance, and integrate the need for security into their overall ethics programs and business processes, they will sensitize their employees to the issues and, by extension, the employees will be more likely to sensitize their family, friends, and other acquaintances. This, over time, should have a positive effect on the culture of society. One other possibility is for companies, through their lobbying efforts, to attempt to influence the legislative and regulatory environment of countries in which they operate to increase the focus on cybersecurity. It is probably naïve to believe companies would avoid doing business in countries lacking strong cybersecurity policies. Rather, profit motives would probably drive them to do business while attempting to take extra precautions to mitigate the increased cybersecurity risk.