The Politics and Policies of Enhancing Trustworthiness

Marjory S. Blumenthal

Computer Science and Telecommunications Board and MIT (1998)

INTRODUCTION

Trustworthiness has emerged as a major policy issue for the next century—although how to define it remains as much a challenge as how to act. It is a creature of the evolving information infrastructure, itself the union of multiple technologies and industries associated with computing and telecommunications (and "information") epitomized by the Internet. Attention to trustworthiness reflects the acceleration of activity to develop and leverage information infrastructure. Under the rubric of "electronic commerce," numerous businesses and personal activities are making greater use of computers and networks that are interconnected, programmable, widely accessible, and designed increasingly for a mass market—what are known as commercial off-the-shelf (COTS) systems. This behavior raises questions for the public and policy makers about what it means to designate a system as "infrastructure," the actual or perceived dependence thereon, and the risk exposure of valuable information relating to persons or property. Concerns about those questions spawned the current crusade for "critical infrastructure," which tempers the enthusiasm about information infrastructure with concerns about its trustworthiness. These concerns are complemented by those relating to the Year 2000 problem, which is less speculative and even scheduled.

"Trustworthiness" embraces security, reliability, safety, and privacy, each of which embraces sets of concepts and controversies, can be addressed separately (recognizing where there is interdependence), and can inspire separate policy principles and debates. Emphasis on specific concepts varies among communities and with circumstances. Making information (and communications) systems more trustworthy implies increasing the likelihood that they will do what they are supposed to do and also that they not do what they are not supposed to do. Uncertainty and therefore how much confidence one can have in an assessment of a system is key to understanding trustworthiness. The intrinsic nature of

information systems, their growing complexity, interconnection, and susceptibility to intentional meddling mean that trustworthiness cannot be guaranteed 100%.[1] Solutions involve technology, people, and policy.[2] Systems problems in general are hard, and trustworthiness problems are especially hard.

Security (i.e., communications security, computer security, and the combined information security) has contributed several sets of concepts for analyzing and addressing trustworthiness: vulnerability, threat, and attack relate to the translation between potential for problems (vulnerabilities and threats) and their exploitation by malicious people (attacks); confidentiality, integrity, and availability are qualities of the information and system to be protected; prevent, detect, and recover, along with the more specific prevent, insure, and self-insure, relate to strategies for coping with problems and managing risk. Other key concepts include accountability, authorization, and monitoring.

One of the reasons for dissatisfaction with trustworthiness policy is that it has emphasized security aspects of problems and solutions. Security tends to emphasize concern with the weakest component and with malice; “attack” and “threat” evoke malice, although as information security jargon threat can include unintentional problems. Trustworthiness is more holistic.[3] The contrast may be most evident when considering the reliability dimension of trustworthiness. Reliability embraces environmental and inherent sources of problems that can be subjected to probabalistic analysis (unlike malicious behavior). In the COTS context, reliability has improved through market mechanisms, at least for system hardware.[4] The comprehensive character of trustworthiness makes it a more useful lens through which to see the big public policy picture than information warfare, which tends to emphasize security and military concerns at least by connotation, or intellectual property protection and electronic commerce, which tend to emphasize commercial concerns.

This paper outlines major issues and provides some historical context in the interest of motivating more and better analysis of trustworthiness policy. It was motivated by the discussions at the 1997 Telecommunications Policy Research Conference session on information warfare, which were constrained by negative reaction to the language of the speakers, who emphasized both security concepts and military concerns. It describes challenges and trends in trustworthiness policy, raising issues relevant

to telecommunications policy. There is more attention to security, which has dominated trustworthiness policy history, than on information policy (e.g., privacy), which is assumed better understood among telecommunications policy researchers.

SIZING UP THE TRUSTWORTHINESS PROBLEM

Security, safety, and privacy experts lament the state of trustworthiness today.[5] They criticize the amount and kind of private action taken to increase trustworthiness by either vendors or users of information technology. Identified problems persist, only to be exploited again and again, and known fixes are not deployed. These circumstances are demonstrated repeatedly in the context of the Internet and COTS systems. The growing scale of deployment and use of information systems appear to compound the problems.[6]

The experts had cautioned that the national or global information infrastructure could not take off without adequate protections, but obviously it has. A variety of publicized surveys report citizen concern with on-line privacy, but use of the Internet continues to grow and diversify.[7] So who is right: Chicken Little or Alfred E. Neuman ("What, me worry?")? How the problem is diagnosed will affect preferences for solutions: experts typically favor prophylaxis, and pragmatists (like most users) appear to emphasize coping strategies. Assuming that experts will continue to recommend more or less ideal solutions, it is important to understand what is feasible and practical.

Diagnosing the trustworthiness problem, in particular its magnitude, is one of the biggest challenges for enhancing trustworthiness. Experts agree that security, at least, must be assessed relative to circumstances (what are the threats) and consequences (what is at stake). To caricature, there is a difference between threats to national security and nuisance-level threats to home PCs—although broadening interconnection and resorting to common technologies blurs some of the differences—and actions taken should be commensurate with such differences.[8] Regardless of circumstances, understanding the magnitude and dimensions of the problem is constrained by lack of information about vulnerabilities and, in particular, threats and attacks. There is more (and perhaps better) information

about problems relating to national security, since the government collects and analyzes intelligence data, than about problems with personal and commercial/organizational systems, for which reluctance to report is well-known.[9] National security concerns overall have become more ambiguous with the end of the cold war, although terrorism appears to be increasing.[10] On the commercial side, there is information about "public" telecommunications service trustworthiness through news coverage and mandatory reporting to the government about significant outages. Regardless of industry or sector, expertise in any aspect of trustworthiness—and especially information security—remains scarce.

Lack of information contributes to limited awareness of problems, which limits the market for solutions. Customers do not demand trustworthiness consistently (other than reliability, at least for hardware), and vendors do not offer much, either because of perceived demand or limitations to their own expertise. Yet the repeated finding that even military systems are inadequately protected raises questions about how much emphasis to place on imperfect information as a problem, at least for information security.[11] Given the propensity across sectors to be reactive rather than proactive on balance, and given that protections may impose immediate and enduring costs, are people and institutions being rational, given the costs and benefits they perceive and given that the worst scenarios remain speculation? Would more and better information make a difference—would it induce a better market outcome? And would the impact of better information be worth the cost of getting it? How people respond to the comparatively well-understood Year 2000 problem, where the "whole world is watching" for costs and consequences, will be an indicator.

An interesting perspective on awareness comes from emerging patterns of interaction between vendors and users of COTS systems. Vendors, and perhaps even users, appear to expect that the systems they offer will be imperfect (more thoroughness is too time-consuming in fast-paced markets and more effort does not guarantee that all problems will be caught), and they rely on users to help them to trouble-shoot. This process can be implicit, as evidenced by the iterative improvements provided in successive versions of a computer system, or explicit, as evidenced by offers of reward to individuals who "break" a system. Vendors thereby externalize part of the process of making systems more trustworthy—in the

process perhaps lowering expectations of their customers about the degree of trustworthiness to expect while keeping purchase costs lower than what they might be with more effort applied prior to sale. For telecommunications and other service providers, cost pressures associated with competition and diminished regulation appear to have fostered a lower, more COTS-like standard of care that is offset by periodic public, including regulatory, scrutiny.[12]

The phenomena above attest to relatively casual practice in developing and deploying the software that is becoming so pervasive in the economy.[13] They also correlate with the limited acceptance of or adherence to expert guidelines for developing more trustworthy systems (except where required by law or regulation).[14] Although non-experts have difficulty appraising some dimensions of trustworthiness, notably security, there has not been strong demand for systems evaluated against criteria advanced by government units, or even for some commercially developed product standards, even among military purchasers. Vendors have complained about the nature of criteria, difficulties implementing them (including development and evaluation delays), and lack of demand for evaluated systems; criteria developers have sought to improve the criteria and evaluation schemes over time. Again, the question must be asked, are people and institutions being rational, given the costs and benefits they perceive? Is it possible to promulgate better-accepted criteria and evaluation schemes?

Another factor in vendor conduct may be the transition from a marketplace characterized by a small number of companies having a history of doing business with the federal government and some openness to discussion with federal officials about security concerns. Diversification of the information infrastructure and entry by a variety of information goods and services providers has brought into the market firms that are either relatively young and/or lacking in history or motivation for cooperating with the government. On the other hand, it has also brought an increase in publicity about problems.

As the observations about awareness and hacking suggest, trustworthiness depends heavily on people: system developers, administrators, and users. People with both deep and limited understanding of a system can injure it. The interplay of people and technology is becoming more complex with the growing interconnection of systems (“private” and “public”), including the interconnection of

organizational and personal systems. The more open systems become, the less it seems possible to depend on having a boundary defense or the comfort of a defined user group.[15]

The role of people, regardless of how automated is an information system, accounts for the importance of policies within organizations about how and by whom information and systems should be handled.[16] Institutional policies codify procedures and, ostensibly, best practices; they may draw on guidance from relevant professional organizations, since enforcement if not framing of these policies tends to engage people responsible for security, privacy, and/or risk management within their organizations.[17] These policies relate typically to privacy and security but may also bear on safety and reliability.

Efforts to enhance public policy both build on and contribute to organizational policy. For example, law and regulation provide incentives to organizations to develop and refine internal policies for employee behavior. The 1990s' rise in law enforcement activity is consistent with the growing exposure of the public to malice involving information systems; it shows the limits of calls by professional societies and trade associations for more ethical behavior in the use of systems.[18] Another example is the development of institutional policies for patient data privacy in health care, which is complemented and influenced by state and federal policy making relating to medical privacy.[19] Like health care but with a longer history, internal banking policies and practices complement federal law and regulation; they also embody a culture characterized by risk management.

Finally, people factor into the trustworthiness equation via attitudes and psychology (e.g., perceptions, public confidence). This is the colloquial concept of trust.[20] It is this aspect of trustworthiness that is most dependent on information, per se—how much and what quality individuals have (awareness).

PUBLIC POLICY ROOTS

Public policy for trustworthiness builds on multiple roots and branches that have developed at least somewhat separately, drawing on the executive branch, congressional inquiry and action, and

independent regulatory agencies. Those relating to information security color strongly the total picture, in part because security contributes to other elements of trustworthiness—security mechanisms can protect privacy, safety, and reliability, for example—and in part because national security is such a dominant policy force. Nevertheless, it is the growth of other kinds of concerns that makes this area of policy particularly rich. A further source of interest is the international nature of trustworthiness concerns, given the international reach of different kinds of communications networks and information systems. Although much of the discussion here is U.S.-centric, the author recognizes that resolution of several problems depends on international coordination and agreement. Bilateral and multilateral discussions appear to be proceeding in connection with all aspects of trustworthiness policy, furthered by controversies over cryptography and electronic commerce policies.

Information Security

Policy relating to information security (which combines communications and computer security) has been driven by national security concerns. The benefits of intelligence data and analysis and of expertise in technologies for cryptography are offset by a command and control orientation and preference for secrecy that contribute to private-sector discomfort with or distrust of military experts in information security. All of these attributes are found in the lead agency for information security, the National Security Agency (NSA), an agency that has sought to change and reach out more to the private sector over the last couple of decades. NSA remains afflicted with a serious image problem. This is due, in part, to its focused national security mission, which calls for it to be able to break as well as protect systems. That seeming conflict has been epitomized in controversies relating to cryptography policy.[21] Cryptography is central to actions individuals and organizations can take to protect themselves—self-protection by the good guys—whereas national security and law enforcement concerns argue for limiting access to cryptography by the bad guys. The result has been a history of controls on the export of cryptography (and other security-relevant technology) aimed at limiting availability and use of this technology in other countries by parties that may be hostile to the United States.[22]

In the 1980s, NSA established an outreach organization, the National Computer Security Center (NCSC), that was responsible for promulgating the Trusted Computer Security Evaluation Criteria (TCSEC)[23] and the associated Trusted Product Evaluation Program (TPEP). The NSA and NCSC's scope grew with the 1984 National Security Decision Directive 145 to include civilian government and some private sector activities, only to shrink with the Computer Security Act of 1987 and the 1990 revision of NSDD 145, which emphasized NSA's focus on classified information and national security government systems.[24] Resistance to the TCSEC and to the next major NSA external initiative, the 1990s Multilevel Information System Security Initiative (MISSI) program,[25] commercial complaints about export controls, and constrained communication about its preferences and processes limited the effectiveness of the NCSC, which was scaled back in the 1990s.[26] More recent NSA outreach has included participation in such external organizations as the Internet Engineering Task Force (to which it contributed work on a cryptographic protocol, ISAKMP), as well as efforts to become more visible (e.g., via the World Wide Web). It has allied with the National Institute of Standards and Technology (NIST) on a new Trust Technology Assessment program to "transfer the evaluation technology in TPEP at the lower levels of trust to commercial laboratories" and a National Information Assurance Partnership to promote testing and evaluation in the private sector.[27] NSA has a history of dominating collaborations with NIST because of its technical and financial resources. With more resources for NIST and a different political climate, these new programs might be more balanced.

Broadening use of information systems and strengthening of mass-market cryptography have stimulated law enforcement involvement in cryptography policy. The Clipper Chip initiative of 1993, the Communications Assistance for Law Enforcement Act (CALEA) of 1994, and late 1990s legislative efforts relating to government access to encryption keys have showcased law enforcement concerns for access to digitally stored and communicated information (and raised questions about common cause between law enforcement and national security interests); the prime exponent has been the Federal Bureau of Investigation (FBI). Law enforcement actions have introduced new concerns about controls on the domestic development and use of cryptography. These potential concerns have provoked outcry by

civil libertarian and other advocacy groups, trade and information technology professional associations, and individual companies that provide computing and communications goods and services. Of relevance to future policy, that outcry has motivated the launch of new advocacy organizations and activities, most recently the Americans for Computer Privacy organization and its advertising campaign. The surge in advocacy has also been fed by broader concerns about privacy and free speech in electronic communications.[28]

The cryptography controversy underscores a structural problem in trustworthiness public policy: there has been no government entity with formal responsibility to protect civilian information infrastructure. The new Critical Infrastructure Assurance Office, discussed below, is a partial response to this perceived need to protect civilian infrastructure. NIST within the Department of Commerce comes closest and therefore is often presumed to have responsibilities that it does not have; neither does it have resources for a broader mission. Other candidates include the Office of Management and Budget (OMB) and the security-oriented National Laboratories operated under the Department of Energy's (DOE) aegis. Like NIST, they focus on the federal government to the extent their missions address security and other elements of trustworthiness, although the National Laboratories also do some projects for industrial clients.

NIST hosts the Computer System Security and Privacy Advisory Board, which considers issues across the economy, and it is responsible for sensitive but unclassified information systems within the federal government, both responsibilities established in the Computer Security Act of 1987.[29] It produces Federal Information Processing Standards (FIPS) and it promotes private sector evaluation of compliance with standards (National Voluntary Laboratory Accreditation Program[30]) in areas that relate to security issues; these efforts are sometimes adopted by the private sector (e.g., FIPS defining the Data Encryption Standard and its implementation). NIST has contributed to the Internet Engineering Task Force Internet Protocol Security (IPsec) effort (e.g., by developing a World Wide Web-based interoperability tester).

Information Infrastructure Initiatives

The National Information Infrastructure initiative launched in 1993 served to define a vision for information infrastructure across the economy. The initiative catalyzed public and private exploration of several issues, including those relating to trustworthiness. It was expanded to refer to a *Global* Information Infrastructure, featuring international discussions and demonstration programs via the G7/G8. It was succeeded by the electronic commerce initiative (discussed below) and the Next Generation Internet (NGI) initiative (in which trustworthiness contributes technical objectives).

The interagency Information Infrastructure Task Force (IITF), active primarily through 1994-1996, led the NII/GII initiative. It was organized into a Telecommunications Policy Committee, Information Policy Committee (IPC), and Committee on Applications and Technology, which included a Technology Policy Working Group; there was also a cross-cutting Security Issues Forum (SIF). The IPC (led by OMB officials) generated principles (and later options) for privacy and intellectual property protection, the SIF generated security tenets, and other IITF components addressed interoperability and other issues that bear on trustworthiness. It provided some support for progress in the development of more trustworthy COTS technology, as part of its broad support for improvements (via research, development, and deployment) in computing and communications technology and system interoperability. Its concern for standards was complemented by private sector activities that have continued to grow.[31] In all cases ideas were circulated for comment, building on and generating public discussion. More ideas were floated than translated into action.

The IITF accentuated the positive. It focused overall on how to broaden access to the infrastructure, but its broad scope and approach to information infrastructure assured that related policy was defined to embrace trustworthiness in the large. Its emphasis on commercial deployment and use was complemented by attention to the policy framework for private action in areas such as information security and privacy where the policy framework focused on behavior within the government. It also furthered consideration of trustworthiness in the context of federal information systems, in conjunction with parallel efforts to strengthen the nature and management of those systems. The IITF spawned what continues as the Government Information Technology Systems Board, and during this period, OMB

revised circular A-130, which provides guidance to agencies on trustworthiness and other requirements for federal information systems, and the vice president organized the National Performance Review initiative to modernize federal agencies. This internal strengthening (like today's Year 2000 response) should, at a minimum, contribute to policy-makers insights into the challenges of making organizations and systems more trustworthy.

Although the IITF did not become engaged in the contemporaneous Clipper Chip cryptography controversy, the NII/GII initiative embraced discussions of public key infrastructure (institutions and systems for distributing and managing cryptographic keys by trusted third parties). The electronic commerce initiative has been intertwined with (and somewhat hamstrung by) the ongoing cryptography controversy. It has furthered policy discourse, emphasizing market solutions, on privacy, intellectual property protection, and security.

Also relating to the realization of an NII are the activities of the Federal Communications Commission's (FCC) Network Reliability and Interoperability Council (NRIC).[32] Established in 1992 as a federal advisory committee in the wake of major network outages circa 1990-1991,[33] the predecessor Network Reliability Council engaged network service providers in the monitoring, study of, and mitigation and prevention of outages. Its charter was expanded in 1996 to include interoperability (including investigations of standards-setting and barriers to interconnectivity and interoperability) with the recognition that the information infrastructure involves multiple kinds of networks and service providers (and in response to requirements of the Telecommunications Act of 1996). By providing a forum for discussion and analysis, the NRIC has provided a kind of government-supervised self-help system as well as advice to the FCC and industry.

Not surprisingly, the NRIC 1997 final report emphasized private sector and market resolution of issues, through such means as standards-setting, activities by such industry groups as the Alliance for Telecommunications Industry Solutions (which established a Network Reliability Steering Committee and has a Network Interconnection/Interoperability Forum), and bilateral negotiations between interconnecting providers covering the specifics of interconnection and interoperation. Consistent with its

roots in telephony and the objectives provided in Section 256 of the Telecommunications Act of 1996, the NRIC called for more and better planning of the evolution of network services, specifically a national planning process that would assure that certain services are available throughout the interconnected network system. It also linked reliability and security to telephony business concerns such as local number portability and toll fraud.

The NRIC 1997 report is interesting for how it characterizes and seeks to balance multiple elements of trustworthiness. It echoed the finding in earlier reports that the dominant source of telecommunications outages is damage to physical facilities, notably cable cuts, which can be mitigated by consultation between construction firms and facilities owners—a good illustration of the roles of people and (procedural) policies and the impact of problems not caused by malice. It expressed concern about how broadening interconnection makes the public telephone network more vulnerable and how, other things equal, deregulation increases security risks.[34] It recommended action to control access to network facilities to alleviate such risk; access control and associated authentication, system audit, and intrusion detection activities are staples of information security. It also linked these issues to national security and emergency preparedness in telecommunications.

National Security/Emergency Preparedness

A major link between conventional telecommunications policy and trustworthiness lies in national security/emergency preparedness programs (NS/EP). Although born of national security concerns, these programs were strengthened at the time of divestiture out of concern for the impact of deregulation on the public telecommunications network (the public switched telephone network). For example, the National Security Telecommunications Advisory Committee (NSTAC), which engages 30 senior corporate executives from telecommunications, computer, and systems integration businesses, was established in 1982 by executive order as a response to then-pending deregulation and divestiture. Its mission includes assessing vulnerabilities and emerging threats and introduction of new technologies into

telecommunication networks.[35] The NS/EP arena also engages state and local interests and actors, as does crisis management generally.[36]

NSTAC provides advice to the president and to the National Communications System (NCS), a Department of Defense organization launched in the 1960s following the Cuban missile crisis to foster interconnectivity and survivability of systems supporting critical government functions during emergencies. The NCS NS/EP mission was expanded in 1984. It engages 23 federal organizations (military and civilian), provides for communication between industry and government and between national governments for purposes of planning and coordination, oversees the Federal Telecommunications Standards Committee, and administers the Telecommunications Service Priority system for priority restoration and provisioning of services during emergencies. It is parent to the National Coordinating Center for Telecommunications, an industry-government entity formed to handle emergency telecommunications requests.[37]

The shift from a narrow concern with the public switched telephone network to the broader information infrastructure has led NS/EP organizations to broaden their own activities. NSTAC has established task forces and working groups to explore relevant concerns, for example. A recent NSTAC report acknowledged bilateral and multilateral agreements among carriers as elements of planning and performance in disaster recovery: "The vast majority of telecommunications disruptions that require a multi-carrier/vendor response effort are addressed through industry cooperation."[38] However, it also noted that there is no experience with and no set of mechanisms for dealing with widespread multi-carrier outage. Further, the government capabilities, including the authority of an often-unfilled position at the FCC, the Defense Commissioner, to support private action under such circumstances are ambiguous. Resulting uncertainty among service providers about their ability to act in an emergency (in ways that may be inconsistent with prevailing law and regulation) may impede timely response.

The NS/EP experience seems to affirm the value of having forums for communication and cooperation within industry and communication between government and industry on telecommunications trustworthiness issues. NSTAC and NCS are among the vehicles that do this,

complementing arrangements among private sector parties; major Internet Service Providers already communicate informally for troubleshooting, and might be integrated into a larger scheme. Although NRIC provides complementary benefits, it operates with much less in the way of organization and resource support—the greater support enjoyed by NSTAC and NCS reflect their links to national security. Experience with these entities should contribute to future efforts to foster cross-enterprise and cross-sector communication and cooperation relating to trustworthiness. However, because the NS/EP activities have been specialized and small in scale, broadening or generalizing its concepts and institutions may be impractical.

Critical Infrastructure

The critical infrastructure initiative of the late 1990s blends information security, national security/emergency preparedness, and at least the information security aspects of the NII/GII initiative and its progeny. As described below, critical infrastructure has led to presidential action because "It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. . . ."[39] In some ways, critical infrastructure responds to the initiatives that promote information infrastructure as a call to caution, balancing the benefits of global reach with domestic if not international protection. It represents a new attempt to frame the trustworthiness problem and integrate military and commercial concerns. Its rhetoric seems to acknowledge the unpopularity and limited success of initiatives focused on information security, per se, and more overtly associated with the military. "Information warfare," with its offense and defense modifiers, is a less neutral-sounding term, and even growing discussion of industrial espionage in the business press does not make IW a term with broad appeal.[40] It was no surprise to the author during a fall 1997 discussion to hear a defense official praise the choice of the term "assurance" in new activities and documents associated with critical infrastructure because of that term's ambiguity to most people (notwithstanding its specialized meaning to information security specialists).

An executive order established the President's Commission on Critical Infrastructure Protection in July 1996 to assess and respond to vulnerabilities and threats across a set of more or less interdependent infrastructures: telecommunications and information services, electric power, oil and gas distribution, transportation, water, banking and finance, emergency services, and government services.[41] In principle, the commission provided a vehicle somewhat outside of the usual decision making mechanisms, but its structure and participation involved substantial participation of information security, national security, and law enforcement players as members, staff, and participants in its steering committee of senior federal officials. It had difficulty engaging senior industry executives as members, but it engaged an industry leader advisory committee and conducted a number of public (industry and citizen) outreach efforts during its working period and after releasing its report.

The commission produced an October 1997 report, *Critical Foundations*,[42] which found that while today there is "no smoking keyboard," the time is right for public and private action because of falling cost and increasing availability of "attack capability" (skills and tools). PCCIP's report emphasized, explicitly and implicitly, the lack of good information on various aspects of trustworthiness. It asserted that the private sector has an important role in collecting and sharing information about vulnerabilities, threats, and attacks—both public and private sectors depend on private sector information about vulnerabilities, threats, and attacks. Arguing that risks are shared across sectors, the report called for public-private partnership. It also pointed to the role of the legal system in providing a framework for action affecting both sectors. *Critical Foundations* was not an isolated statement: in the same time frame, the White House, via the Office of Science and Technology Policy, issued a descriptive (and motivational) document entitled *Cybernation* emphasizing reliability.[43] Also, NSTAC and NRIC reports were published in the commission's working period, and the broad scope of PCCIP contributed to interest and activity by a variety of industry organizations in that period.

The PCCIP release yielded modest publicity and a stream of intra-government discussions about next steps. Most notable in its aftermath, a May 1998 presidential decision directive, PDD 63,[44] established goals that cut across sectors and levels of government and a new bureaucracy.[45] The

Department of Commerce is the lead role for the information infrastructure generally and the Department of Defense, via NCS and NSTAC, for NS/EP aspects. The NSA was directed to continue to assess risks to federal systems; the Departments of Commerce and Defense and the General Services Administration to help federal agencies implement best practices; and OMB to consider aspects relating to the Government Performance and Results Act.[46] In addition, there is a parallel complex of private sector participants, and a private-sector-driven Information Sharing and Analysis Center is called for.

At the hub of the new bureaucracy is the Critical Infrastructure Assurance Office (CIAO). CIAO responds to the PCCIP recommendation for a national focal point to provide public awareness and meet specific federal government needs and is consistent with recommendations flowing from the contemporaneous NSTAC assessment. In conjunction with CIAO, the FBI was directed to expand its warning organization to a full-scale National infrastructure Protection Center.[47] The Department of Defense has also moved to set up an organization under the Assistant Secretary for Command, Control, Communications, and Intelligence responsible for critical infrastructure protection.[48] Both PCCIP and CIAO link clearly national security, law enforcement, government requirements, and economic security.[49] In short, comprehensive and powerful action is enabled, although at this point all that is evident are plans and structures.

POLICY THEMES

Notwithstanding softness in conceptual frameworks and increasingly contentious politics, two themes emerge from contemporary policy-making in trustworthiness: private-public partnership and the search for a better institutional approach.

Public-Private Partnership

A call for public-private partnership is the central theme in trustworthiness policymaking, most notably in the information security and critical infrastructure arenas. “Partnership is the foundation for infrastructure protection” is a slogan of PCCIP. Beginning with the NII/GII policy thread, there has been

growing acknowledgement of the politics and interest-balancing required with a predominantly privately owned information infrastructure. For information security specifically, the IITF 1996 Security Task Report, for example, took the position that the federal government can support the private sector, and it acknowledged private sector concerns about the structure and conduct of federal security policy.[50] The NII initiative sought to raise consciousness and promote some societal consensus on relevant issues, and this tack is echoed in the White House *Cybernation* document, which acknowledges business interest in reliability, as well as the White House *Global Framework for Electronic Commerce*.[51] These developments mark progress from the initiation of the NCSC, which indicated that even a historically secretive agency needed to reach out to industry to address the information security problem affecting both military and civilian activity. The NII initiative also underscored the value of leadership action (role modeling) on the part of federal agencies. The opportunity for leadership (and the potential for control) was echoed in the establishment of CIAO.[52]

PCCIP called for promoting voluntary cooperation and maintaining existing oversight and regulation while suggesting strongly the potential for new administrative structures that might lead to new regulation. The white paper accompanying PDD 63 and establishing CIAO continues this theme.[53] As stated in *Cybernation*, "Neither the private sector nor the government can completely address infrastructure reliability alone."

In contrast to computer systems companies aversion to centralization, telecommunications (and especially telephone) companies associated with NRIC contributed to the recommendation for national coordination and planning of a minimal set of "national services." Existing such services (dial-tone, 800/888 number service, e-911) reflect industry-led planning. NRIC and subsequent NSTAC discussion of these services noted that service providers (i.e., industry) must work to define the services and relevant standards, in cooperation with such agencies as NCS and users.

Fundamental to all of the proposals for partnership and cooperation or coordination is enhanced flow of information. Trustworthiness experts recognize that the information base includes anecdotes but little data, making it difficult to gauge the nature and level of threat, let alone what is an attack.

Cybernation called for "[a]n equitable, institutional means, within clear statutory limits, for the timely two-way flow of relevant intelligence information and incident data between government and the public utilities…" (p.3). Even though there is broad agreement on a need for awareness and education, there is less agreement on the need or willingness of private parties to supply information that might make education and awareness promotion credible. NSTAC, for example, noted that banks and financial institutions were leery of new reporting requirements on top of current ones.[54] Part of industry's concern relates to the history of limited access to government information on the basis of national security classification.

PCCIP took the tack of exhorting cooperation for mutual benefit, but questions arise about incentives and about actions (mandates) if incentives do not work. These concerns are shaped by an adversarial history relating to export controls, and they are heightened by observations of law enforcement movements on the legislative front via possible modifications to CALEA and new legislation relating to encryption.[55] Regardless of whether law enforcement actions are interpreted properly, cooperation and partnership will require trust among the parties and genuine evidence of mutual benefit.

New Institutions?

The evolution of trustworthiness policy shows a continuing search for the how as well as the what to do. The launch of CIAO represents the latest attempt to pursue a bigger and broader agenda via a new institution. It reflects a history of frustration epitomized by the launch, modification, and effective resorbing of the NCSC by NSA, the resource- and mission-driven constraints on NIST, and the focused or specialized missions of other federal agencies (e.g., Defense Advanced Research Projects Agency, FCC, DOE, NCS, OMB). During the NII/GII initiative heyday, some comic relief was provided by the retraction of a report that a new federal agency was being proposed "to help secure and police the nation's growing 'information highway.'"[56] According to the retraction, "the proposals were meant to 'stimulate a dialogue' on how the federal government would work with state and local governments and the private sector on setting up such an entity." Does CIAO signal that the dialogue has taken place?

One concept for a new entity has undergirded considerable discussion during the 1990s, including by PCCIP. In 1991, the National Research Council's Computer Science and Telecommunications Board issued the report, *Computers at Risk*, which called for a new organization (the Information Security Foundation (ISF)) that would promulgate expert guidance (Generally-accepted Systems Security Principles) and provide information and education services. It noted the limitations of existing public and private sector organizations, the inherent difficulties of working within—and with—the federal framework, and the perils of becoming captive to vendors. The authoring committee did not prescribe fully how to structure and situate the ISF; it noted that private sector activities were growing in the area of security but leadership was needed to address the broader set of problems posed by trustworthiness. These perspectives remain valid today.

The ISF concept has triggered a variety of exploratory efforts, beginning immediately with two years of discussion and planning by the predecessor of the Information Technologies Association of America and follow-on activity by an arm of SRI International (I-4) with a history of information security activity. This was followed by exploration over the past several years by NSTAC and the Information Technology Industry Council, which formed in 1997 at NSTAC's request the Information Security Exploratory Committee (ISEC).

ISEC's mission focused on private sector assesment of the NSTAC proposal inspired by the ISF called the Information Systems Security Board (ISSB), which also received support from some government officials. ISEC concluded in a January 1998 statement that an information and awareness program is needed, and that it should be undertaken by a private non-profit Information Security Foundation to be sponsored by the ITIC. This ISF would be smaller in scope than the ISSB or originally proposed ISF, which ISEC characterized as a "centralized body" focused on standards-setting and other activities already underway in the private sector; it would focus on educational programs. The ISEC position reflects resistance to the concept of a new entity that could constrain private action.[57] Such resistance is consistent with collective action on specific issues, which range from cryptography policy to setting standards for conduct relating to handling of personal information.[58]

Taking a more centrist position, the IITF Security Task Report called for an Information Technology Security Policy Issues Clearinghouse that would match industry needs and questions with government security groups. It argued that a no existing entity could or should play this role.[59]

CONCLUSION: CAN POLICY BE HOLISTIC?

Like other kinds of policy, policy relating to trustworthiness requires choices and tradeoffs.[60] These are evident for each dimension of trustworthiness and become more complicated with a holistic perspective. Although the dimensions of trustworthiness are complementary and can often be fostered with the same or similar technical mechanisms, differences in the nature, culture, and maturity of policy-making for each dimension hinder an integrated, holistic approach to policy. As the issues have become clearer and more numerous, inconsistencies have become more obvious and calls for a focal point louder. None of this means that a comprehensive strategy is workable from a political and/or public administration perspective.[61] The question "Who's in Charge?" will likely endure for the foreseeable future.

The Computer Security Act of 1987 seems prescient for its attention to both privacy and security and its sensitivity to contrasts between civilian and military perspectives and needs associated with information and systems.[62] A decade later, the Federal Trade Commission's activity in on-line privacy policy illustrates how change relating to information security may arise from nontraditional players. Whereas the Computer Security Act focused on the Departments of Defense and Commerce as actors and on problems within the federal government, in mid-1998 the FTC proposed legislation (absent satisfactory self-regulation by industry) that would require compliance with "widely-accepted fair information practices" including notice/awareness, choice/consent, access/participation, and security/integrity. The last would provide that "Web sites would be required to take reasonable steps to protect the security and integrity of that information."[63]

The 1990s have seen progress in institutional structure for information security and privacy, which varies in treatment by industry.[64] A fragmented approach also characterizes safety and reliability.

These latter dimensions would appear to achieve greater prominence under the critical infrastructure rubric, but the actual treatment seems narrow. For example, safety aspects of software in medical devices, addressed by the Food and Drug Administration, might not be covered by CIAO, although safety aspects of software in transportation or nuclear power plants might. The FCC enters into the safety and reliability arena piecemeal and sometimes in ways that may conflict with privacy, such as a new requirement for emergency 911 location-tracking for mobile telephone users.[65] Nevertheless, a comprehensive and uniform approach is premature at best. Accordingly, the FTC's proposal for privacy legislation anticipated that implementation would vary by industry and with technological progress.[66] Also, the PCCIP/CIAO processes suggest continued examination of issues within industry contexts over the near term.

The combination of information (content) and systems (the nature of the technology and services) in trustworthiness complicates the policy picture. Information security and NS/EP policy have tended to focus on the technology and service, per se; privacy policy places emphasis on the information; and information warfare considers information—"perceptions management" and deception, the manipulation of trust—in addition to system security and reliability. Space precludes consideration of the issues, but it is not hard to see that a variety of issues relating to information policy could bear on trustworthiness.[67] At the intersection of these areas are the growing value of information, the potential for technology to separate ownership from access or use, and consequences of alternative patterns in the flow of information—all of which affect tradeoffs.

The body of law (statutory and common) that impinges on trustworthiness and may bridge policy domains is growing. This trend is unfolding almost apart from the administrative action and programs that seem to dominate information security, NS/EP, and cryptography policy. It is consistent, however, with information policy, which is characterized by legal framework and dispute resolution.

Defining what constitutes criminal activity is an ongoing process, often advancing as a result of specific case experience. Early law relating to computer crime and to privacy focused on federal information systems, whereas more recent action addresses systems across the economy.[68] In the wake of

the 1988 Internet Worm, the Computer Fraud and Abuse Act helped to clarify the criminal nature of some kinds of activity, and a computer crime unit was established in the Department of Justice and soon expanded to include related intellectual property protection. As debate over legislative proposals for intellectual property protection illustrates, imperfect understanding of computer systems yields language that would outlaw common, inoffensive conduct.

The incidence of computer-related crime has been growing, evident in corporate espionage and hacking and extending to organized crime and crimes against children. Information systems can be a target of crime, an instrumentality, or a repository or vehicle for evidence relating to crime. They can magnify the scale and impact of crime, and they pose challenges relating to anonymity, jurisdiction, and evidence. Because information infrastructure transcends national borders, harmonization of laws internationally and cooperation in law enforcement are increasingly important and presuppose examination within each country.[69] National assessments are colored by judgments relating to international competition in a world of electronic commerce.

While what is wrong is being defined by law, ambiguity persists on private rights. Most notorious, perhaps, is the debate over whether U.S. citizens have a right to privacy; there is a related debate regarding anonymity.[70] Trustworthiness policymaking reinforces these debates, because of new concerns about how law enforcement will be conducted and at what cost to such other trustworthiness concerns as privacy. Industry advocates and cyberlibertarians argue for a private right of choice for information technology, including private choices about technology for trustworthiness. For example, the Computer Systems Policy Project advanced the security principle that system users have a right to choose the mechanism and the strength for protecting information security.[71]

Defining civil and criminal liability generally affects entry into and conduct within information systems businesses, and it influences the behavior of people as they design and use information systems. For example, resolution of liability issues is key to progress in public key infrastructure and the institution of related certificate authorities;[72] different liability issues are associated with warranties for software, at issue in the private sector-driven efforts to update the Uniform Commercial Code.[73] The Year 2000

problem has propagated attention to cyberlaw issues across the legal community, contributing to growth in private sector attention and activity relevant to trustworthiness. An American Bar Association committee concerned with electronic commerce has even proposed a new kind of job, the cybernotary, which would combine legal and computer security expertise to assist in network-mediated transactions.

The FTC's late 1990s actions regarding on-line privacy and consumer fraud (in connection with Year 2000 impacts on goods and services, Internet advertising, and use of the Internet for "a new generation of fraud that uses increasingly sophisticated technology") hint at more regulation or enforcement activity.[74] The FTC is motivated in part by concern about exploitation of children, a lightning rod in the development of Internet policy. It has been evaluating industry actions, noting that there are three kinds of mechanism to back up privacy principles: self-regulation, private remedies (as established by law), and government enforcement.[75] New action, echoing policy development for intellectual property rights, would be based either on extrapolation of existing rules or development of new ones for electronic media, as well as more aggressive education aimed at both industries and consumers.[76] Analogies and differences between the Internet and telephony are being explored.[77]

Although policy making relating to critical infrastructure and privacy protection suggests attempts to be proactive, the body of law and policy in the United States generally favors a more reactive and private-sector-based (e.g., via contracts and/or litigation) handling of problems. As suggested earlier in this paper, trustworthiness issues force questions about the merits of ex ante vs. ex post action. The costs of regulation are well known to economists; the question within the trustworthiness domain is whether one can establish that the risk of substantial and irreparable harm justifies intervention. Again, the Year 2000 experience will be telling: forecasts of high levels of private litigation are consistent with expectations that the private sector can resolve most issues, and reports that specific industries—notably the same set as critical infrastructure—are undertaking extraordinary prophylaxis is also consistent with private sector responsibility (albeit under public sector scrutiny). The mid-1998 interpretive release of the Securities and Exchange Commission (SEC) establishes a broad requirement for public companies to disclose their Year 2000 readiness, costs associated with inadequate readiness, risks, and contingency

plans.[78] The actions of the SEC, another nontraditional player, illustrate the potential to build on conventional business mechanisms (others beside disclosure include auditing and insurance) to promote trustworthiness, and the facilitation of private action by reinforcing accountability.

The combined body of policy affecting trustworthiness will influence information system design. That interaction has been the focus of cryptography policy controversy (policy calling for law enforcement access to information would affect the nature of commercial systems) and emerging information policy developments. Failings of past approaches to technology (notably the goal of the TCSEC, "trusted systems") and criticisms of new approaches (e.g., the World Wide Web's Platform for Privacy Preferences or the Secure Electronic Transaction protocol for credit cards) have been linked to failings in the models and policies being implemented—and to attempts at one-size-fits-all solutions. Public-private partnership sounds like it could yield consensus, but is elusive. New institutions appeal when old ones fall short, but offer no guarantees. Getting trustworthiness policy right will continue to be a process for the foreseeable future.

END NOTES

The author is grateful for comments on an earlier draft provided by Peter G. Neumann and Willis Ware. Responsibility for the content remains hers.

[1] Accordingly, federal support for research into more trustworthy computing and communications systems has proceeded recently under the label of "high confidence systems." Note that guarantees or expectations presuppose testing, and inasmuch as intentional meddling is a factor it may be especially hard to figure out what to test for.

[2] Key concepts and technology attributes and issues are described in a 1998 report of the Computer Science and Telecommunications Board, *Trust in Cyberspace.* National Academy Press, Washington, D.C., and a 1991 CSTB report, *Computers at Risk: Safe Computing in the Information Age.* Those reports contain numerous references.

[3] Through the 1980s, a criticism of the military approach to security was its emphasis on confidentiality relative to integrity (then of at least as great concern in industry) and availability. Today, there appears to be broad recognition of the importance and interdependence of all three aspects, and growth in networking has amplified concern with availability.

[4] In the larger information infrastructure, questions persist about the sufficiency of market mechanisms for promoting this and other dimensions of trustworthiness; analogies are drawn by some to public-sector intervention where safety is at risk (e.g., food and drug systems, nuclear power and transportation systems), and major outages prompt public scrutiny and various interventions.

[5] These concerns recur in congressional hearings, government reports (see, for example, the 1998 Office of Science and Technology Policy report, *Cybernation*, the 1996 Defense Science Board report on *Information Warfare—Defense*, and assorted critiques by the congressional General Accounting Office on federal agency problems relating to security, privacy, and reliability).

[6] Documentation is provided through the various writings of Peter Neumann, moderator of the on-line RISKS Digest and author of the 1995 book *Computer-Related Risks*, ACM Press, New York.

[7] "When eight out of ten Net users (81%) say they are concerned about threats to their personal privacy when using the Internet, it is clear that this is not an issue worrying only the 'Privacy Paranoid' or 'Net Libertarians.' At the same time, the fact that only 6% of Net users say they have ever personally been the victim of an online privacy invasion shows that it is primarily

anticipatory concern and responses to privacy-threat stories in the media not actual experiences and online annoyances." Louis Harris and Associates, Inc., and Dr. Alan F. Westin. 1998. "E-Commerce & Privacy: What Net Users Want (Executive Summary)." Sponsored by *Privacy & American Business* and Price Waterhouse LLP, June, www.aba.com).

[8] Relativity is not limited to active threats. For example, FDA attention to software in medical devices varies with what the software is supposed to do. See Center for Devices and Radiological Health. 1998. "Guidance for FDA Reviewers and Industry: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices." Food and Drug Administration, U.S. Department of Health and Human Services, Rockville, MD, May 29.

[9] Much attention was paid to delayed publicity about an incident affecting Citicorp because it dealt with a real and significant incident. See Carley, William M. and Timothy L. O'Brien. 1995. "How Citicorp System Was Raided and Funds Moved Around World." *The Wall Street Journal*, September 12., p.A1, p.A18.

[10] See Winter, Tim. 1998. "U.S. Spy Agencies Find Scant Peril on Horizon." *The New York Times*, January 29, p.A3.

[11] The Computer Security Act of 1987 called for federal agencies handling sensitive information to prepare computer security plans. Subsequently it was recognized within government that neither the formulation nor the implementation of those plans was adequate, notwithstanding the law's call in addition for security training. More recently, funding by agencies of an organization designed to monitor and assist in response to civilian agency system problems was reported to be jeopardized by lack of agency appreciation for threats and attacks. See Harreld, Heather. 1997. "Security team in money crunch." *Fderal Computer Week*, December 1, p.10, p.14.

[12] See the 1989 Board on Telecommunications and Computer Applications (CSTB) report, *Growing Vulnerability of the Public Switched Network*, and the 1997 report of the Network Reliability and Interoperability Council, discussed later in this paper.

[13] This situation sets the stage for problems associated with mobile code, which although not new have grown with broader internetworking. See *Trust in Cyberspace*. Note also the tradition emphasizing disclaimers by independent vendors rather than strong warranties. The Year 2000 situation has focused some attention on this practice by both large purchasers of software and by such regulatory agencies as the Federal Trade Commission (see, for example, "'Year 2000' Consumer Issues; Request for Comment," *Federal Register*, 63:87, May 6, 1998, pp.25045-25-49.)

[14] Beginning with the U.S. Trusted Computer Systems Evaluation Criteria, the past two decades have seen a series of governmental and private sector discussions across countries about how to define what it takes for a system to be secure at a given level and what it takes for evaluation against those criteria to be itself trustworthy (i.e., must a government or government-controlled entity conduct the evaluation). See *Trust in Cyberspace*, and "Common Criteria for Information Technology Security Evaluation, May 1998, Version 2.0, CCIB-98-026, available at www.nist.gov. More recently, regulatory attention to software has grown in agencies with safety missions, including the Food and Drug Administration (which has been developing standards for software in medical devices), the Federal Aviation Administration (which has been developing standards for reliable air traffic control software), and the Nuclear Regulatory Commission (which has been developing standards for software in nuclear power plant control). Note that most industry standards relate to interoperability of systems; security experts are also concerned about assurance, for which it is harder to make specifications or conduct tests.

[15] There is ongoing research into technical mechanisms to respond to the reality that either information or systems with which one interacts may not be trustworthy, although most research to date has been shaped by models that assume more control. In today's marketplace, firewalls, at the boundary between trusted and untrusted networks, are a common if imperfect response to the imperative for external connection. See *Trust in Cyberspace.*

[16] One source of criticism of the TCSEC relates to its underlying security models and policies; see *Computers at Risk* and *Trust in Cyberspace*.

[17] There are general practitioner professional groups, such as the Information Systems Security Association, and specific ones relating to specific fields, some of which may be more properly classified as trade associations (e.g., American Bankers Association).

[18] The 1988 Internet Worm led to a spate of efforts to promulgate codes of ethics. Meanwhile, the proliferation of computer viruses, reports of system break-ins, and hoaxes about viruses and other problems point to the growing recreational value of tampering with systems. Also, there has been growth of academic centers that attack systems as part of their research (e.g., Princeton University Secure Internet Programming Laboratory: "We are studying the security of widely-used Internet software, especially mobile code systems like Java, ActiveX, and JavaScript. We try to understand how security breaks down, and to develop technology to address the underlying causes of security problems." (http://www.cs.princeton.edu/sip/))

[19] See Computer Science and Telecommunications Board. 1997. *For the Record: Protecting Electronic Health Information*. National Academy Press, Washington, D.C.

[20] It is illustrated by a recent examination of banking that noted that "financial institutions actually value customer confidence more than the customer's money, which affirms the axiom in banking that the only things banks really sell is trust." See National Security Telecommunications Advisory Committee. 1997. *Reports Submitted for NSTAC XX* (Volume III: Financial Services Risk Assessment Report), Washington, D.C., December 11.

[21] See Computer Science and Telecommunications Board, Kenneth Dam and Herbert Lin, eds. 1996. *Cryptography's Role in Securing the Information Society (CRISIS)*. National Academy Press, Washington, D.C.

[22] Of course, part of the challenge to export controls comes from parties that assert that foreign availability from other sources vitiates controls; the governmental response is to ascertain whether foreign-source technology is truly comparable to controlled U.S. technology, which may not be obvious on the surface.

[23] U.S. Department of Defense. 1985. *Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, Washington, D.C., December. See *Computers at Risk* for an assessment.

[24] According to the committee report accompanying the Computer Security Act of 1987:
"One reason for the assignment of responsibility to NBS [now NIST] for developing federal computer system security standards and guidelines for sensitive information derives from the committee's concern about the implementation of National Security Decision Directive-145. As indicated previously, this directive established an interagency committee--the National Telecommunications and Information Systems Security Committee (NTISSC) [now NSTISSC]. The function of the NTISSC is to devise operating policies needed to assure the security of telecommunications and automated information systems that process and communicate both classified national security information and other sensitive government national security information. Policies developed by NTISSC would apply government- wide.

"While supporting the need for a focal point to deal with the government computer security problem, the Committee is concerned about the perception that the NTISSC favors military and intelligence agencies. It is also concerned about how broadly NTISSC might interpret its authority over 'other sensitive national security information'. For this reason, H.R. 145 creates a civilian counterpart, within NBS, for setting policy with regard to unclassified information. In so doing, the bill has the additional effect of specifically limiting the purview of the NTISSC to systems containing classified information and cancelling[sic] the authority contained in NSDD-145 for systems containing unclassified information. NBS is required to work closely with other agencies and institutions, such as NSA, both to avoid duplication and to assure that its standards and guidelines are consistent and compatible with standards and guidelines developed for classified systems; but the final authority for developing the standards and guidelines for sensitive information rests with the NBS."
See http://csrc.nist.gov/secplcy/csa_87.txt.

[25] MISSI sought to propagate the Fortezza key-accessible cryptography system.

[26] Security criteria tend not to be fully explained, out of expert concern about the perils of broadcasting information about vulnerabilities, threats and attacks. Computer scientists often challenge this approach by noting the benefits of openness: broader testing and analysis increases the likeliness of problems being found and fixed. Repeated reports of security flaws are broadening this debate. See Caruso, Denise. 1998. "Digital Commerce: As long as software code is kept secret, Internet security is at risk." *The New York Times*, August 17, p.D3.

[27] See www.nsa.gov:8080/isso/brochure/prodeval.htm. The success of the new structures, like their predecessors, is not automatic; as noted about TTAP on Microsoft's Web site, "Getting through this evaluation is a learning experience for both the NSA as well as the product vendors." (http://www.microsoft.com/security/c2summary.htm)

[28] Together, the advocates address both classical privacy (protection of personal information) and confidentiality (relevant to all kinds of information), which can be confused. ACP, for example, focuses on cryptography policy and therefore confidentiality; the Electronic Privacy Information Center focuses more on classical privacy.

[29] As stated in the Act, "The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use." Those practices include standards (FIPS) and plans and programs within federal agencies, both areas where NIST was given a lead. The Act also says that NIST is authorized "to assist the private sector, upon request, in using and apply the results of the programs and activities" under the Act.

[30] See www.ts.nist.gov/nvlap.

[31] For example, the confederated Information Infrastructure Standards Panel has paid special attention to security-related standards, as have such industry groups as the Information Technology Industry Council and the Cross-Industry Working Team and the more broadly composed Internet Engineering Task Force. Specialized groups such as the Smart Card Forum, with focused trustworthiness concerns, also blossomed in this period.

[32] See www.fcc.gov/oet/info/orgs/nric.

[33] For an indicator of public concern and congressional reaction, see Committee on Government Operations. 1991. *Asleep at the Switch? Federal Communications Commission Efforts to Assure Reliability of the Public Telephone Network.* U.S. Congress, House of Representatives, Washington, D.C., December 11.

[34] "The deregulation of the industry, absent security standards and solutions for managing risk in an open competitive unbundled Telecommunications environment, may drive enormous holes in existing security mechanisms and access controls to the executable code of the public network building blocks, network elements, operating systems and data communications networks. While there is a rich, if not open, history associated with the security exposure and risk management of the PTN, the security issues arising from the interconnection of telecommunications networks and systems over the last decade is without precedent. . . . Unlike the Internet and its World Wide Web, notwithstanding the massive Toll Fraud Problem, the PTN has not recognized significant security exposure related to the exploitation and corruption of vlunerable computer and network technology." (section 6.4, pp.107-8)

[35] See National Security Telecommunications Advisory Committee. 1997. *Reports Submitted for NSTAC XX* (Volume I: Information Infrastructure Group Report, Network Group Intrusion Detection Subgroup Report, Network Group Widespread Outage Subgroup Report; Volume II: Legislative and Regulatory Group Report, Operations Support Group Report; Volume III: National Coordinating Center for Telecommunications Vision Subgroup Report, Information Assurance, Financial Services Risk Assessment Report, Interim Transportation Information Risk Assessment Report), Washington, D.C., December 11.

[36] See Computer Science and Telecommunications Board. 1996. *Computing and Communications in the Extreme*. National Academy Press, Washington, D.C.

[37] There is also a Joint Telecommunications Resources Board that convenes agency heads under the director of the Office of Science and Technology Policy to address non-wartime telecommunications needs authorized by executive order.

[38] National Security Telecommunications Advisory Committee. 1997. *Reports Submitted for NSTAC XX* (Volume I: Network Group Widespread Outage Subgroup Report), Washington, D.C., December 11, p.7.

[39] See www.ciao.gov.

[40] See "Despite passage of the 1996 Economic Espionage Act, the FBI says foreign spies have stepped up their attacks on U.S.-based companies…" Reprinted from *Los Angeles Times*, January 21, 1998, at www.infowar.dom/class_2/class2_011498b.html-ssi.

[41] Executive Order 13010.

[42] President's Commission on Critical Infrastructure Protection. 1997. *Critical Foundations.* Washington, D.C.

[43] Like the PCCIP report, *Cybernation* acknowledges that "[m]any of the recognized threats to the information networks supporting the domestic infrastructure have not actually been experienced." (p.2)

[44] See white paper at www.ciao.gov.

[45] "No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."

. . .

"For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies."

. . .

"On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate."

[46] See PDD 63 and "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." "The NSA in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations."

[47] "This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity." Located in FBI headquarters, the center was launched in 1998 with a "mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures." See A Message from Michael Vatis, Chief of the National Infrastructure Protection Center, www.fbi.gov/nipc/welcome.htm.

[48] See Verton, Daniel M. 1998. "DOD preps office for cyberdefense." *Federal Computer Week*, July 13, www.fcw-newscyber-7-13-98.html.

[49] "The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained."

[50] "In 1995, the IITF NII Security Issues Forum prepared the paper "NII Security: The Federal Role . . . Among other things this paper outlines four areas of Federal responsibility for the NII:

- The Federal government will serve as a facilitator and a catalyst for promoting private sector activity.
- In its role as guardian of the public interest and general welfare, the government will cooperate with other governments, the private sector, and the public-at-large in setting legal and policy ground rules for security in the NII.
- The Federal government can support the private sector's development of needed technology by funding research and development in critical areas.
- As a model user of the NII, the Federal government has a responsibility to ensure that its own automated information is secure."

See Technology Policy Working Group. 1996. "Security Task Report: Draft for Public Comment, July 29." http://nii.nist.gov/pubs/sec_task_rpt.html .

[51] "The traditional policy tools available to the government for working with the marketplace to achieve national objectives—including legislation, regulation, licensing, tax and rate-setting regimes, and other inducements—all offer important options in the reliability arena. However, none of them can be effective unless and until there is consensus on what the minimum levels of reliability should be, what the threats are, what risks are acceptable, what protective measures should be taken, and how the costs should be met." (*Cybernation*, p.11) See also White House. 1997. *Global Framework for Electronic Commerce*. Washington, D.C., July 1.

[52] "The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors." Activities in connection with the Year 2000 problem also suggest some potential for the federal government to demonstrate how to be responsive—in addition to its need to attend to its own problems, which have national impact.

[53] " [P]artnership must be genuine, mutual and cooperative. . . . the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector. . . . The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security."

[54] Banks experience regulation, including reporting requirements, that may address security and other trustworthiness issues, from the Federal Reserve Board, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Securities and Exchange Commission, Commodities Futures Trading Commission. Some reporting is considered particularly burdensome, such as that for the Financial Crimes Enforcement Network. The Financial Crimes Enforcement Network, which focuses on money laundering, implements the Suspicious Activity Reporting System.

[55] There were six bills relating to cryptography in 1997 alone. CALEA debates were reopened in 1996 and continue. See, for example, McGee, Jim. 1996. "Heightened Tensions Over Digital Wiretaps." *The Washington Post*, October 27, p.H1, p.H12.

[56] See Fialka, John J. 1995. "U.S. to Propose Data-Highway Agency." *The Wall Street Journal*, June 14, n.p., and "New Agency Won't Police The Information Highway, *The Wall Street Journal*, June 15, p.B7.

[57] The host organization, ITI, also participates in IISP and contributed to that organization's input to the European Commission about security standards. There, too, it was argued that numerous standards-setting activities already exist (e.g., within the International Organization for Standards and the International Telecommunications Union). See www.ispo.cec.be/eif/policy/com9850enhtml.

[58] Note that it is not clear that there is a consistent position in "the private sector" or information technology industries. For example, in 1996, the Cross-Industry Working Team, representing several communications and computing companies, released a statement calling for a Joint Security Technology Policy Board organized as an independent government agency composed of government officials and members of the private sector in equal proportion. See Cross-Industry Working Team. 1996. "A Process for Information Technology Security Policy." www.xiwt.org/documents/SecReportFinal/SecReport.html .

[59] " Examples of coordination issues in security technology policy that the Clearinghouse should be able to address are:

- Cryptographic Technology
- Public Key Infrastructure
- Access Control Systems
- Network Security
- Dual Use Technology
- Technology Research
- Interoperability of Government and Industrial Systems
- Government Technology Transferable to Industry
- Export Controls for Technology
- International Security Technology Policy"

See Technology Policy Working Group. 1996. "Security Task Report: Draft for Public Comment, July 29." http://nii.nist.gov/pubs/sec_task_rpt.html .

[60] The formulation in *Cybernation* is, "How can society be certain that critical infrastructure information networks are reliable enough?" Disagreements about how much is enough are considerable.

[61] On the other hand, some degree of breadth helps to advance debate at a time when cryptography policy narrows discussion and promotes posturing. Although cryptography is important to achieving trustworthiness, and much progress hinges on resolution of cryptography policy concerns, the broader discussion goes far to show why, where, when, to whom, and how cryptography or any other mechanism matters.

[62] It also presented a broad concern for information needing protection; the committee report accompanying the bill summarized an ongoing debate about "sensitive but unclassified information" and offered a definition that included safety, privacy, intellectual property, and other concerns. "Sensitive information is defined as unclassified information which, if lost, misused, accessed or modified in an unauthorized way, could adversely affect the national interest the conduct of federal programs or the privacy of individuals. Examples include information which if modified, destroyed or disclosed in an unauthorized manner could cause:

- Loss of Life;
- Loss of property or funds by unlawful means;
- Violation of personal privacy or civil rights;
- Gaining of an unfair commercial advantage;
- Loss of advanced technology, useful to a competitor; or
- Disclosure of proprietary information entrusted to the government.

The definition of sensitive information allows the possibility that some unclassified information may not be sensitive."

[63] See "Prepared Statement of the Federal Trade Commission on 'Consumer Privacy on the World Wide Web' before the Subcommittee on Telecommunications Trade and Consumer Protection of the House Committee on Commerce of the United States House of Representatives," Washington, D.C., July 21, 1998, www.ftc.gov/os/9807/privac98.htm, and Federal Trade Commission. 1998. "Privacy Online: A Report to Congress." Washington, D.C., June.

[64] According to the FTC, "Current American privacy law can best be described as sectoral, consisting of a handful of disparate statutes directed at specific industries that collect personal data . . ." Federal Trade Commission. 1998. "Privacy Online: A Report to Congress." Washington, D.C., June, endnote 160. Similarly, cryptography policy has involved disparate treatment for banking, and some have speculated that progress may be achieved on an industry by industry basis. See Mosquera, Mary. 1998. "Encryption Resolution May Be Sector By Sector," *TechWeb*, July 30, http://pubs.cmpnet.com/internetwk/news0730-1.htm, and Clausing, Jeri. 1998. "Administration to Allow Limited Data-Scrambling Exports." *The New York Times*, July 8, www.nytimes.com/library/tech/98/07/biztech/articles/083ncrypt.html.

[65] See Markoff, John. 1998. "Finding Cellular Callers in an Emergency." *The New York Times*, August 17, p.D5. The FCC enforces legislative protections of customer-proprietary network information, and its rules affect Caller-ID and ANI services provided by telephone companies.

[66] Several industries have moved to promote privacy, responding both the U.S. and European policymaking developments. For example, the American Bankers Association, Consumer Bankers Association, and Bankers roundtable have developed privacy principles for the banking industry (see www.aba.com); as has the Securities Industry Association for that industry (see www.sia.com/html/privacy_protection.html), which asserts that "[g]iven the breadth of its curent regulatory regime and its history of, and self-interest in, protecting the privacy of investors, the industry believes proposals to impose uniform privacy standards throughout the private sector are premature."); and a variety of associations representing property/casualty and life insurance companies (see www.aiadc.org/euprivacy062298.html).

[67] Solutions in information policy tend to be less technological than security solutions.

[68] The Counterfeit Access Device and Computer Fraud Act of 1984 was amended by the Computer Fraud and Abuse Act of 1986 (PL 99-474) and concerned with "federal interest computers."

[69] Note that international law relating to information warfare appears particularly ambiguous. "Perhaps because of the newness of much of the technology involved, no provision of international law explicitly prohibits what we now know as information warfare. This absence of prohibitions is significant because, as a crudely general rule, that which international law does not prohibit it permits. . . .," (p.17) Greenberg, Lawrence T., Goodman, Seymour E., and Kevin J. Soo Hoo. 1997. *Information Warfare and International Law*. Command and Control Research Program and National Defense University, Washington, D.C.

[70] See, for example, Froomkin, Michael A. 1996. "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases." *University of Pittsburgh Journal of Law and Commerce*, 15 (395).

[71] Computer Systems Policy Project. 1996. "Perspectives on Security in the Information Age." Washington, D.C. January. See www.cspp.org.

[72] See, for example, Kent, Stephen. 1997. "How Many Certification Authorities Are Enough?" MILCOM '97, Monterey, CA, November 3-5.

[73] Current efforts to revise section 2B of the UCC, according to public interest advocates, may protect vendors more than consumers. Criticisms are poted at www.badsoftware.com.

[74] The IITF's work is cited heavily by the FTC, which characterizes the history of privacy principle development and the legal framework for privacy protection. See Federal Trade Commission. 1998. "Privacy Online: A Report to Congress." Washington, D.C., June.

[75] See Federal Trade Commission. 1998. "Privacy Online: A Report to Congress." Washington, D.C., June, pp.10-11.

[76] See "Interpretation of Rules and Guides for Electronic Media; Request for Comment," *Federal Register*, 63:87, May 6, 1998, pp. 24996-25006; "'Year 2000' Consumer Issues; Request for Comment," *Federal Register*, 63:87, May 6, 1998, pp.25045-25-49; and Federal Trade Commission. 1998. "Fighting Consumer Fraud: New Tools of the Trade." Washington, D.C., April. According to the latter publication, "Consumers and commercial marketers are not the only groups to see the value and power of the Internet. Con artists also are online…" (p.3).

[77] In the consumer fraud area the FTC has examined the applicability of 900# disclosure rules to the Internet, for example.

[78] The SEC has been issuing Year 2000 guidance since at least 1997. See Securities and Exchange Commission. 1998. "Interpretation; Statement of the Commission Regarding Disclosure of Year 2000 Issues and Consequences by Public Companies, Investment Advisers, Investment Companies, and Municipal Securities Issuers." Release Number 33-7558, Washington, D.C., July 30 (Effective August 4) at www.sec.gov; and Gibson, Dunn & Crutcher LLP. 1998. "SEC Issues Release Providing Additional Guidance on Year 2000 Disclosure Obligations." Washington, D.C., August 17.