(U) The National Computer Security Center and the Origins of NSA's Information Assurance Mission

~~(U//FOUO)~~ Evan Rea and Kara Smit

(U) Computers came into widespread use in the late 1950s and 1960s. With them came the myriad possibilities offered by automated data processing (ADP) as well as the need to ensure that the information computers stored and manipulated stayed secure. This realization led to many attempts over the years to understand and define the requirements needed to keep data safe. The Department of Defense's journey to protect computers and the information inside them is a story told by acronyms: from *ADP* to *DoD CSC* to *NCSC* and then to *IAD* before finishing (for now) in *CSD* and *CCC*.

(U) The Department of Defense Computer Security Center (DoD CSC) began the task of establishing computer security standards for the DoD. The CSC then became the National Computer Security Center (NCSC), responsible for computer security standards government-wide. While the transformation from identifying the need to beginning to fill that need crawled for almost 30 years, the following two decades spent trying out various fixes sped by until the NCSC faded into NSA's Information Assurance Directorate (IAD) by 2000. The problem had not gone away—it had just been reconceived. Whereas DoD once saw data security as primarily a hardware problem, the department ultimately realized that computers had to be secured in a cyber matrix. That realization helped give rise to US Cyber Command, NSA's Cybersecurity Directorate (CSD), and CSD's new Cyber Collaboration Center (CCC), the heir to the DoD CSC and NCSC.

(U) Setting the Stage

(U) Recognizing the need to protect data, Congress held a series of hearings on computer security, beginning with the 1966 House Special Subcommittee sessions on "Invasion of Privacy." The subcommittee's concern lay in finding ways to protect personal data inside computers. Representative Frank Horton (R-NY) described the problem of collecting personal information in databases during a session on July 26, 1966:

> Good computermen know that one of the most practical of our present safeguards of privacy is the fragmented nature of the present information. It is scattered in little bits and pieces across the geography and years of our life. Retrieval is impractical and often impossible. A central databank removes completely this safeguard.[1]

Representative Horton was referring to a proposal to establish a national data center of personal information for the US Census Bureau—a proposal that the government and the research community liked, but the general public viewed with apprehension. Arguments against the national data center were based on the difficulty of ensuring that the information collected in computers remained secure and safe from misuse. That concern would take root in the government and evolve over the next decade and a half.[2]

(U) Recognizing that computers were there to stay as part of the federal government, Congress had already passed the Automatic Data Processing Act of 1965, which amended the Federal Property and Administrative Services Act of 1949. Called the Brooks Act after its chief sponsor and advocate, Representative Jack Brooks (D-TX), the legislation gave the General Services Administration responsibility for purchasing and management of ADP equipment government-wide, as part of an ongoing effort to reduce costs. The Brooks Act implicitly took the position that all ADP systems essentially performed the same types of functions, implying that unless there was a genuine requirement for specialized components, it was more efficient and frugal to have one central authority for procurement.[3]

(U) Meanwhile, within the DoD and the realm of classified national security data, computer systems were becoming more prevalent as intelligence operations rapidly began relying upon them. More computers led to recognition of the need for computer security as a new "pressing issue within the Department of Defense."[4] Adding to the sense of urgency was the 1970 Ware report, prepared for DoD's Defense Science Board (DSB). Dr. Willis Ware of the RAND Corporation pointed out that computer security was a new field, and this report "was the first attempt to codify the principles and details of a very involved technical–administrative problem."[5] Ware knew that a time-sharing, multi-access computer system was vulnerable—he would later say that "the only completely secure computer was one that no one could use"[6]—but that very connection allowed resource-sharing, which in turn allowed computers to be more cost efficient. This vulnerability required a solution to protect privacy and secure data. The report, therefore, highlighted the immediate need for "a technical agent … to establish procedures and techniques for certifying security controlling systems, especially the computer software portions and for actually certifying such systems."[7]

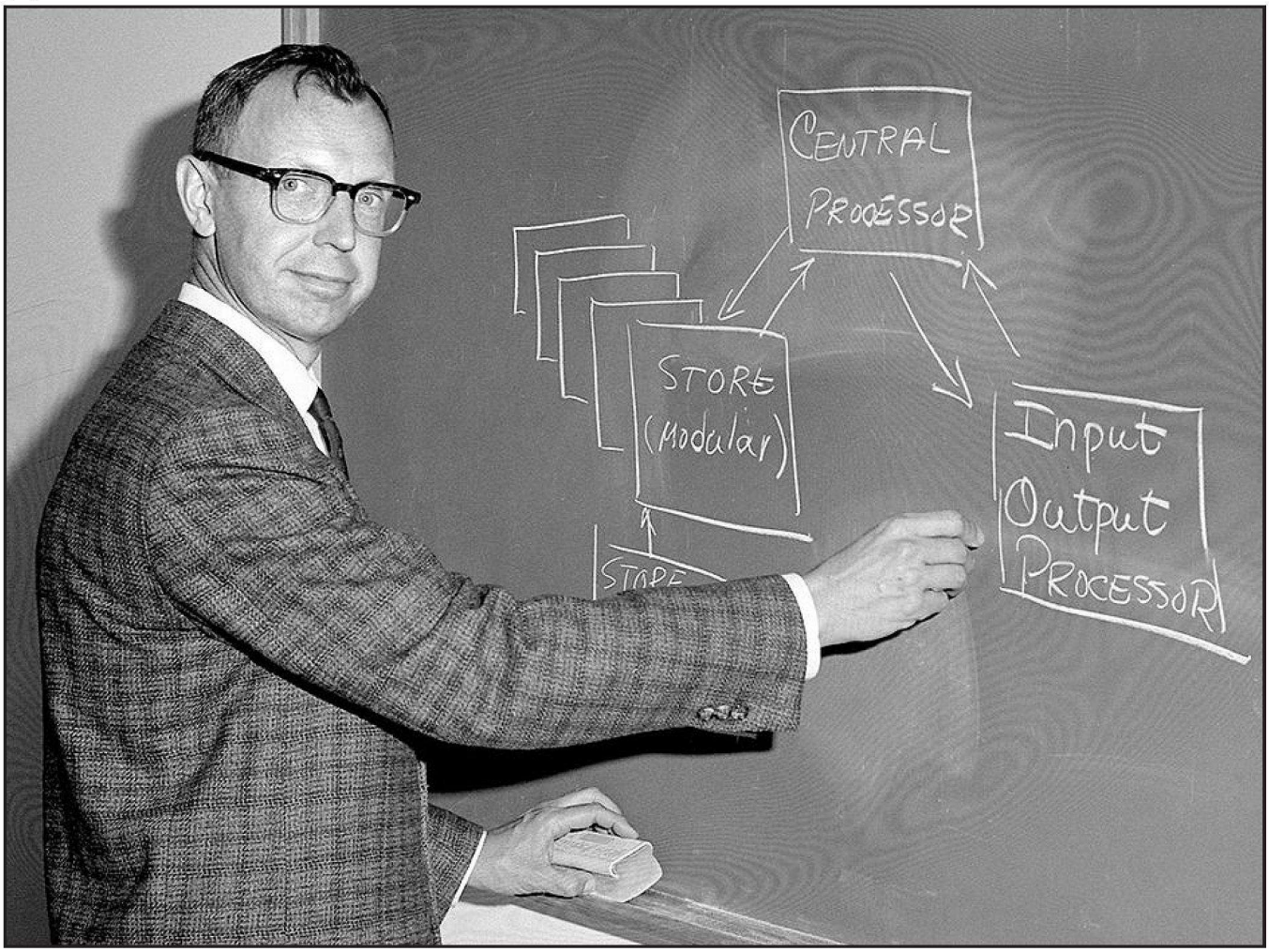
(U) Ware's report clarified the problem and identified the way forward. Classified and compartmented information created unique challenges and requirements for system security that did not exist elsewhere in the US government. Solving that issue created friction with the Brooks Act and its emphasis on economy, which would take decades to resolve.

(U) The Concept for Solving the Issue

(U) Directly after the Ware report's release, the DoD established an ADP Security Task Force to improve computer security. The task force's remit was to review and identify needed changes to security policy directives to use advanced technology in ADP systems. This charter, along with the Ware report, "shifted emphasis to the task of developing practical, realistic policy on a Department-wide basis,"[8] which was a significant undertaking at that time. One part of their solution was DoD Directive (DoDD) 5200.28, issued in 1972, which built upon the Ware report's suggestions.

(U) DoDD 5200.28 established policy for protecting classified information stored and processed in an ADP system, standards for physically protecting those systems, and requirements for testing and evaluating the hardware and software security features of those systems.

(U)



(U)

(U) Dr. Willis Ware, 1962. Ware wrote a key report for DoD's Defense Science Board. NSA photo

Subsection IV.B of the directive called for the assistant secretary of defense for administration (ASD [A]) to establish "a central DoD capability" to assist and advise DoD components in ADP security testing and evaluation, as well as assess the progress of DoD components as they developed and installed effective ADP security. (DoDD 5200.28 did not specify how the central capability was expected to assist components nor did it specify where that capability should be located.) In essence, this was a call for a center for computer security to craft standards and guidelines within the DoD.

(U) Interestingly, while Subsection IV.F.2 required DIRNSA to provide communications security assistance to the DoD components, it also specifically prohibited NSA from evaluating, approving, or validating ADP systems not related to NSA's mission and functions. That prohibition could have been due to the requirement in IV.G.1, stating that the director of the Defense Intelligence Agency (DIA) would accredit "the

compartmented security mode of ADP systems of DoD components and their contractors, except for systems under the cognizance of the NSA," while the director, Joint Staff would accredit and authorize waivers for ADP systems handling compartmented classified material.[9]

(U) The DoD and the intelligence agencies' growing dependence on computer systems was an obvious driver for enhancing ADP security, but certain events highlighted challenges, defined systems of the era, and exposed limitations. One of the Intelligence Community's (IC) first interagency computer networks, the Community Online Intelligence Network System (COINS), began in 1965 as an experimental file-sharing system. Led by NSA and DIA, COINS consisted of independent file storage systems at geographically separate IC agencies linked to a central switch (located at DIA). The central switch and supporting hardware allowed analysts from one agency to query and retrieve data from another agency's linked system. Although primitive by today's definition of the term, COINS was a rudimentary computer network that passed data from one machine to another. And with that came the fundamental concerns of ADP security, such as preventing unauthorized access, data loss, and spillage.[10]

(U) A separate but related issue, which had existed from the very first discussions on computer security in the IC, was multilevel accreditation.[11] This referred to a computer system that processed varying levels of classification (Top Secret, Secret, Confidential, and compartments), while keeping the levels separate *and* ensuring users could only access information for which they were cleared. Multilevel accreditation was an essential issue at that time because computers of that era were large, expensive, centralized mainframes that had to support multiple users simultaneously (a shared-resource system). Such flexibility for users would make those installations—in 1964 an IBM System/360 could cost $2,700 to $115,000 a month to rent or $133,000 to $5.5 million to buy—much more cost efficient.[12]

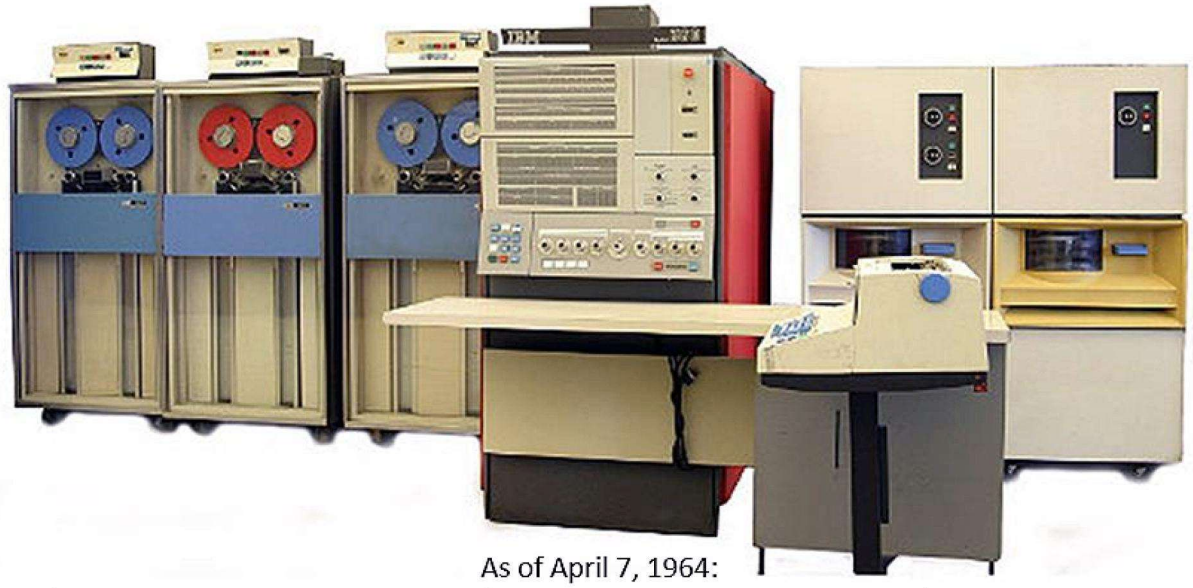
(U//FOUO) DIA's COINS file storage system was known as the ANalyst Support and Research System (ANSRS), which was replaced by the DIAOLS (DIA On-Line System) in 1971. In 1969, DIA proposed using ANSRS as a testbed to establish the necessary criteria, techniques, and safeguards to enable multilevel security accreditation in the IC. The testing would involve participants from across the IC so that they could apply lessons learned to achieve multilevel accreditation for their agencies' systems. DIA made thorough preparations for the test, compiling an impressive array of testing data, which showed that the software and administrative safeguards were comprehensive and reliable. In essence, DIA dared the IC to test the security of DIAOLS.[13] Test (or tiger) teams were composed of personnel from the IC, DoD, and contractors, who were organized by functional area (personnel security, physical security, procedural security, communications security, software, hardware). James P. Anderson was one of the contractors involved, an ominous sign for DIA. Anderson "wrote the book"—or rather the report—on computer security for the US Air Force: "Computer Technology Planning Study," released in 1972.[14]

(S//REL) The tiger teams concluded their DIAOLS testing in August 1972. Anderson and his tiger team colleagues gained control of DIAOLS from a remote terminal, while one team member accessed the DIA computer building using a counterfeit badge. (Since he was there, the intruder also attempted—and succeeded—in accessing COINS. He was never challenged.) Undaunted, DIA was set to try again in 1974, though this time NSA declined to participate. In the end, DIAOLS continued to operate at a "system high" level: all people, places, and things associated with the system met the security

(U)

IBM System/360

A single system spanning the performance range of virtually all current (1964) IBM computers
Includes in its central processors 19 combinations of graduated speed and memory capacity.
Core storage memory capacity ranges from 8,000 characters of information to more than 8,000,000.



As of April 7, 1964:

System/360 monthly rentals ranged from $2,700 for a basic configuration to $115,000 for a typical large multisystem configuration. Comparable purchase prices range from $133,000 to $5,500,000.

In 2023 dollars, that would be $26,141.07 to $1,113,415.86 for monthly rental, or $1,287,689.64 to $53,250,323.62 for purchase.

(U)

(U) IBM System/360. Photo by C. Mark Richards

requirements of the highest level of intelligence information processed by that system. The fact that many classified networks—including those at NSA—continue to operate at a system high points to the enduring challenge of multilevel security. The DIAOLS testing is also instructive because of what it revealed: in those early days, a network of computers was still viewed as a collection of machines, and efforts to secure it focused on securing the individual parts, not the whole.[15]

(U) Knowing the results of the DIAOLS testing, and as the agency considered most knowledgeable about securing data, NSA first floated the idea of becoming the DoD central technical authority in 1974. Then-director of NSA (DIRNSA) Lt Gen Lew Allen, USAF, corresponded with the assistant secretary of defense (comptroller) (ASD [C]), stating that NSA was "qualified to take on the central technical capability role for ADP security within the DOD." He

also noted that a "significant part…of total system security for ADP will involve COMSEC considerations and techniques. Furthermore, privacy methods and technical safeguards will be partially dependent upon cryptographic approaches." Since both COMSEC and cryptography were already under NSA's purview, Allen wrote that it was in the best interest of the DoD to make NSA the technical authority for ADP. (Allen's quote is telling of the technological situation at that time. COMSEC measures could only protect what went into or came out of a computer—not what was inside. The concept of hardware that could secure computers at a network level was more than a decade away.)[16]

(U) The response was not what Allen expected. The ASD (C) pointed to the provisions of DoDD 5200.28, specifically those in Subsection IV. "The central technical capability was envisioned as an advisory role," ASD (C)'s response explained, and each DoD component would have the delegated authority "to evaluate the ADP systems within their jurisdiction and determine whether or not the system was in compliance with DoD policy."[17] In addition, a draft memo sent by the office of the ASD (C) to the chair of the Joint Chiefs of Staff (CJCS), agency directors, and other staff for review said that:

> The Navy, NSA, and DIA are each capable of providing a central technical capability, but are not recommended since we believe that they lack the necessary authority and influence over other DoD components to accomplish the stated management objectives. Further, the secretive nature of the NSA and DIA missions causes concern when considering the requirements of the Privacy Act.

In short, the Pentagon told NSA and the other agencies that their leadership was not required. The idea of a central body for DoD computer security would not begin to take shape until the end of the decade.[18]

(U) NSA would soon be distracted by yet another looming issue—the prospect of the Soviets intercepting US government phone conversations in the United States. Not only did the Soviets target the government's microwave communications, they targeted defense contractors' communications as well.[19] In response to this threat to national security, President Jimmy Carter released Presidential Directive-24 (PD-24), "Telecommunications Protection Policy," in 1977. PD-24 established the National Telecommunications and Information Administration (NTIA) and its Special Project Office (SPO) under the Department of Commerce. Established in 1978, the SPO was tasked with protecting government-derived unclassified information unrelated to national security as well as commercial and private sector communications. The SPO was expected to work with NSA to accomplish that task.[20] The relationship, however, did not go well. This was partly due to the SPO's lack of both budget and expertise. NTIA had already started phasing out the SPO; it would be completely gone by the end of 1983.[21] As then-DIRNSA VADM Bobby R. Inman, USN, later said, "competence wasn't available that could be hired on the street…NSA [had] a monopoly of talent."[22] The problem of data security was about to go global.

(U) Mr. Walker's Winding Road to the Computer Security Center

(U) Around this time, one individual became the driving force for the creation of a computer security center for DoD: former NSA employee Stephen T. Walker. The Advanced Research Projects Agency (ARPA, now known as the Defense Advanced Research Projects Agency [DARPA]) hired Walker in 1973 to manage a computer security program. He established the ARPA Technical

Working Group (TWG) for computer security in 1975. Walker then moved on to the Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence (OASD C3I) in 1977, under Dr. Gerald P. Dinneen. Walker recreated the TWG as the Computer Security Technical Consortium in March 1978. Later in 1978, he established the Computer Security Initiative (CSI), with the goal of increasing the availability of trusted computer systems. This meant commercially developed and commercially available secure ADP systems capable of being used simultaneously for multiple levels of classified and sensitive information.[23] The CSI, in cooperation with the National Bureau of Standards (NBS, under the Department of Commerce), sponsored a series of computer security conferences. They provided a forum for government, commercial, and private sector computer security experts to exchange ideas and foster the development of trusted systems.[24] Leading experts in computer security along with representatives from well-known corporations such as IBM, Honeywell, RAND, MITRE, and Sperry-UNIVAC took part in CSI and the annual computer security conferences.

(U) In 1979 Walker joined a project to plan a computer security evaluation center that would establish the central DoD technical authority for ADP. In contrast to the earlier ideas discussed above, he proposed that the new center be run as a program management office (PMO) at NSA and report to OASD C3I. This proposal drew objections from other DoD components, which believed that while such a center was necessary, placing it with NSA would be a hindrance. There was "strong feeling among the services that they would be better off if they did not 'let NSA into their knickers,'" and that with NSA there would be "much interference and little immediate help." Cognizant of the resistance, Walker then informally circulated an alternate proposal in February 1980. Walker recognized that computer security was a government-wide problem, not just a DoD matter. Thus, his new plan was for a Federal Computer Security Center located with the NBS in Gaithersburg, Maryland. Still, Walker's preference was to co-locate the proposed center with NSA, due to the Agency's technical expertise. He felt that if the center was located elsewhere, the first question that would come up in any situation would have been, "what does NSA think?"[25]

(U) Assistant Secretary of Defense Dinneen conferred with DIRNSA Inman on computer security topics in April 1980. The two discussed Walker's initial proposal to assign NSA as the DoD's technical authority for computer security. A key aspect of the proposal was to model the evaluation center on the COINS PMO, which had been located at NSA since its start in 1965. NSA leadership, however, did not consider the COINS PMO to be a good model for the center. The primary concern was that COINS did not have strong IC support, despite the fact that it was a joint program. The COINS PMO obtained its staff from NSA personnel, contracts, and R&D projects, and was funded with NSA monies. The proposed computer evaluation center, in contrast, needed to have the full commitment of its participants. When the DoD CSC was established, however, it was intentionally staffed and funded solely by NSA from the beginning.[26]

(U) Dinneen briefed Walker on his meeting with VADM Inman, which led to Walker's concern that DIRNSA had not fully understood the proposal, and was only resistant to the idea of hosting the proposed center at NSA. Walker then requested a meeting with Inman and was prepared to discuss the February 1980 proposal, which placed a federal computer security center with the NBS at Gaithersburg. Ironically, the meeting was postponed due to a serious security mishap with the missile defense computers at the North American Aerospace Defense Command

(NORAD) the day before, on June 3, 1980.[27] Although no information was lost and no missiles were fired, this incident highlighted the decisive position that computer systems already held—and the accompanying risks.[28]

(U) Walker's meeting finally took place on August 4, 1980, when to his surprise, Inman resisted the proposal to locate a federal evaluation center with NBS. "I've had nothing but trouble with those Commerce guys," said Inman, referring to the aforementioned difficulties NSA had with NTIA/SPO. Not only did Inman want the computer security center to be located at NSA, Walker realized, it would be set up as a PMO like COINS. Inman initially wanted to make sure the new center was established as an entirely separate entity from NSA. His concerns were to keep the computer center out of NSA's hierarchy; thus, it would have its own budget and would downplay the perceived influence NSA could have on the center's computer standards. Inman believed that the needs of the government were substantially different from those of the DoD and he could see getting into arguments over standards. Adopting computer security standards that were right for the DoD but too high for other departments would ultimately lead to "systems that were vastly more complex and vastly more expensive than needed" and would have limited commercial use. The meeting ended on a hopeful note for Walker when Inman asked him to send a written proposal for an evaluation center.[29]

(U) Walker subsequently arranged for Dinneen to send Inman the formal request for a computer security evaluation center at NSA, on September 3, 1980. Inman's interest showed in the alacrity with which he responded—his response was dated October 7, 1980. The speed suggested that Inman's prior meeting with Dinneen had been more substantive—and productive—than Walker thought. In fact, unknown to Walker, Inman had consulted his senior staff about a computer evaluation center connected to NSA after his discussion with Dinneen. Many of the details for establishing the new organization (known as C1 and later C) had already been worked out. In addition to programming for funding and staffing, NSA needed to consolidate existing activities involved in providing external support to computer security. This included efforts to develop a COMSEC plan for computer systems (at the direction of the US Communications Security Board), and participation in committees on computer security policy, along with developing standards and techniques for computer security across the federal government. Up to that point, however, NSA had been managing its association with computer security initiatives as opposed to executing assigned responsibilities. That engagement had still been restricted to computer applications that were related to NSA's national COMSEC responsibilities.[30]

(U) In January 1981, after the years of back and forth between NSA and DoD, Deputy Secretary of Defense W. Graham Claytor, Jr., signed the memorandum for a DoD computer center to evaluate computer system and network security. The memo was addressed to leaders in the DoD; among them were the chair of the Joint Chiefs of Staff, secretaries of the military departments, and directors of NSA, DIA, and DARPA. Claytor's memo spoke to all of the addressees directly as he acknowledged their concerns. Despite those concerns, he affirmed the need for a DoD computer security evaluation center:

> Although your comments in response to Dr. Dinneen's memorandum of November 15 indicate some concern about the working relationships within the proposed Evaluation Center, there is no disagreement or doubt regarding the need. Therefore, the proposal made by the Director, National Security Agency to

> establish a Project Management Office is approved. Effective January 1, 1981, the Director, National Security Agency is assigned the responsibility for Computer Security Evaluation for the Department of Defense.[31]

Claytor then called for representatives for computer security matters from each of the addressees to take part in the group developing the center's charter. The center would be responsible for evaluating computer security systems. Shortly thereafter, NSA technical leader and high-performance computing pioneer George Cotter was appointed as the first director of the DoD Computer Security Center (DoD CSC). Cotter would initially act as Walker's point of contact and liaison with NSA.[32]

(U) The CSC and the TCSEC

(U) The DoD CSC was formally established under the new DIRNSA, Lt Gen Lincoln Faurer, USAF, on July 13, 1981. The DoD CSC would "expand on the work of the DoD [Computer] Security Initiative" and "encourage the widespread availability of trusted computer systems" within the DoD.[33] Walker and Cotter were part of the group that wrote DoD Directive 5215.1, "Computer Security Evaluation Center," which became the new center's charter when it was formally issued in 1982.[34] The CSC's key missions hearkened back to James P. Anderson's 1972 report on computer security, which stressed that computer security must be built into a system "at its inception, there are no simple measures later to make it secure."[35] The charter called for the CSC to establish technical standards and specifications for DoD computer systems and network security, evaluate secured systems for DoD components and key contractors, conduct research and development, provide training and guidance to DoD elements and other federal agencies, facilitate the exchange of computer security information, and act as DoD's point of contact for computer security among the government, industry, foreign governments, and the North Atlantic Treaty Organization (NATO).[36] After almost two decades of limiting its external engagement to policymaking and advisory roles, NSA was taking an active, hands-on step into computer security beyond its own walls.

(U) Much of the DoD CSC's early work went into drafting the Trusted Computer System Evaluation Criteria (TCSEC, better known as the Orange Book and part of the Rainbow Series). The TCSEC was developed as a joint computer security community effort, involving computer security experts from across the federal government and various agencies, as well as the private sector. The people who worked on the Orange Book are familiar names in computer security. They included Sheila Brand (as primary author), Dan Edwards, Roger Schell, and Marvin Schaeffer of NCSC; Grace Nibaldi and Peter Tasker of MITRE; and Ted Lee of Sperry-UNIVAC. The reviewers list boasted names that are just as well known and included James P. Anderson, Steve Walker, Clarke Weissman, and Steve Lipner.[37] The TCSEC was initially issued in 1983 as the CSC's first standard: CSC-STD-001-83. The Orange Book was formally adopted by the government in 1985 as DoD 5200.28-STD, "Trusted Computer System Evaluation Criteria,"[38] and completely replaced the directive's initial 1972 issuance. Various volumes of the Rainbow Series were published from the mid-1980s through the 1990s, covering everything from configuration management to networking. These volumes were intended to guide computer manufacturers, software programmers, and government purchasers in producing and purchasing equipment that met the required security standards at various levels.[39]

(U) The scope of CSC's operations expanded in 1985, in response to National Security Deci-

(U)

(U)

(U) The Rainbow Series of books released by the National Computer Security Center over the years. Department of Defense photo

sion Directive 145 (NSDD-145), "National Policy on Telecommunications and Automated Information Systems Security" (September 17, 1984). NSDD-145 replaced PD-24 and represented the first time telecommunications and automated information systems—computers—were addressed concurrently in a presidential directive. NSDD-145 stated that technologic advances spurred growth in the telecommunications and information processing services for the government and the private sector. With these advances, the directive explained, "traditional distinctions between telecommunications and automated information systems have begun to disap-

pear." The directive then warned that "although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges" because:

> Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation.[40]

NSDD-145 assigned responsibility to NSA for developing standards and guidelines protecting sensitive, unclassified data (Sensitive but Unclassified [SBU]) for the entire US government and designated the director, NSA, as the "National Manager for Telecommunications and Automated Information Systems Security."[41] One result of NSDD-145 was a new name for the center: the National Computer Security Center (NCSC). The change "better reflect[ed] its responsibility for computer security throughout the federal government";[42] this included ensuring the security of national computer security systems and "the systems and telecommunications involving classified and Warner Amendment Systems," which were the computer systems related to defense and national security.[43]

(U) Within NSA's Information Security Directorate (DDI), NCSC continued to test and evaluate new systems; it also moved toward identifying existing vulnerabilities. The Computer Security Technical Vulnerability Reporting Program (CSTVRP) of 1986 was the first DoD effort to actively seek out hardware and software vulnerabilities in commercial products used by DoD components. Under CSTVRP, the National Information Security Assessment Center (another organization within DDI) collected vulnerability reporting from computer security teams throughout the DoD elements and transmitted "technical vulnerability information to affected manufacturers for corrective action." The NCSC performed technical analysis of the reported vulnerabilities while also determining the effects each might have on products that the center had previously evaluated. In retrospect, CSTVRP stands as a milestone of information security's growth and evolution. It showed NSA's new commitment to improving the security of military communications, data security across the federal government, and, for the first time, data security within the computer manufacturing industry.[44]

(U) Regulating Computer Security

(U) Representative Jack Brooks had not lost his interest in governmental ADP or fiscal responsibility over the years. He was also suspicious of NSA and its role in computer security. When President Reagan signed NSDD-145, Brooks called it "one of the most ill-advised and potentially troublesome directives ever issued by a president."[45] Not only did the directive place NSA in control of the security for government computer systems, it directed the Agency to review and assess telecommunications systems security programs and budgets of other government departments and agencies. It also allowed NSA to enter into procurement agreements for "technical security material and other equipment"[46]—and to provide that material to other government agencies.

(U) Brooks sponsored the Computer Security Act of 1987 (CSA), which transferred responsibility for protecting federal SBU Information

Technology (IT) to the NBS (which became the National Institute of Standards and Technology [NIST] in 1988). When introducing the act, Brooks referred to NSDD-145, saying that it represented "an unprecedented expansion of the military's influence on our society, which is unhealthy politically and potentially very dangerous."[47] The act required the NBS to work with NSA in establishing the standards and guidelines for protecting government computer systems.

(U) An amendment to the 1965 Brooks Act was added to the CSA in 1988. It became known as the Warner Amendment for Sensitive But Unclassified National Security Systems, and confirmed that the standards and guidelines established in the CSA would be compulsory and binding for federal computer systems. It also established a waiver system for the procurement of computer systems exempted by a previous amendment to the Brooks Act. This earlier amendment was the Warner Amendment of 1981.[48] The 1981 amendment explicitly carved out DoD procurement of ADP equipment and services for defense purposes. In other words, computers used for national defense were not subject to the Brooks Act, and that did not change.

(U) These legislative changes, combined with budget reductions, led NSA to reorganize its communications security and computer security directorates and combine them with the NCSC. With some NCSC personnel now working more closely with NSA, this movement gave an outward appearance that the NCSC had "reduced in staff in the late 1980s."[49]

(U) President George H. W. Bush codified the Computer Security Act of 1987 and the 1988 Warner Amendment[50] into National Security Directive 42 (NSD-42)[51] in 1990. NSD-42 created the National Security Telecommunications and Information Systems Security Committee (NSTISSC) to facilitate discussion and set national policy and to release guidance for the security of national security systems. The CSA defined the role of NBS (later NIST) in protecting sensitive information and limited NSA to its traditional protection of classified information. The NCSC's public presence changed, and its "research and evaluation functions were integrated with the NSA's communications security functions."[52] This gave the appearance that NSA was replaced by other agencies, such as NIST.[53] The Paperwork Reduction Act of 1995, however, reaffirmed NIST's and NSA's separate responsibilities for developing guidelines and standards for different types of SBU IT.[54] The Clinger-Cohen Act of 1996[55] repealed the Brooks Act, although it retained the Warner Amendment restrictions on SBU national security systems. Clinger-Cohen assigned the overall responsibility for acquisition and management of IT in the federal government to the Office of Management and Budget (OMB), while creating chief information officers (CIOs) in each federal department to manage IT. The OMB set the rules to improve acquisition and management of information resources, and the individual procurement departments in the federal government and agencies had to abide by those rules.

(U) NCSC, the Public Face of NSA

(U) As public-facing organizations, the DoD CSC and later the NCSC sponsored annual computer security conferences in nearby Baltimore, Maryland, from 1981 to 2000. The first director of the CSC, George Cotter, was involved in each conference, and successive directors followed his example. As with the Computer Security Initiative conferences, leading experts in computer security participated. Willis Ware and James Anderson, whose early reports on computer security helped create the field, presented papers at these conferences. Cliff Stoll, whose bestselling novel *The Cuckoo's Egg* related his experiences tracking German hackers through American computer

networks, presented papers on the importance of computer security. After the conferences, the NCSC issued proceedings from each event to spread knowledge of the topics discussed.[56]

(U) Public awareness of the NCSC remained limited to people involved in the computer security field, although there are hints that it had a wider reach at times. The December 1990 volume of the journal *Science* said that "between 1983 and 1990, the NSA ran an advisory body 'outside the perimeter' of secrecy." The *Science* article was reporting on a National Research Council study, "Computers at Risk: Safe Computing in the Information Age," that called for the establishment of a private, nonprofit Information Security Foundation. While the NCSC had been a good solution, the article noted, by 1990 it had "[gone] back behind the wire of secrecy." The NCSC's computer security standards and service as a research hub, the article went on, had offered "a valuable service for the handful of companies…that wanted to develop defenses."[57] *PC Magazine* described the NCSC's function as "to support standards and evaluation of computing technology for secure applications by government agencies."[58]

(U) By the late 1990s, however, complaints were rising, as well as calls to update the Orange Book criteria. The world had gone online with the Internet revolution, and federal government buying power no longer allowed Washington to dictate ADP standards as companies competed for growing global markets. Information technology and information assurance methodologies evolved quickly, and the TCSEC was too rigid and limited in scope to keep up. The process of getting equipment and software through NCSC inspections was lengthy and expensive, leading to products rendered obsolete before gaining certification. Vendors also preferred the efficiency of international criteria rather than dealing with multiple criteria from separate nations.[59]

(U) The End of the NCSC

(U) The work of the NCSC continued as part of NSA's Information System Security Office until 2000. Two in-house programs—the Trusted Product Evaluation Program (TPEP) and Trusted Technology Assessment Program (TTAP)—handled evaluations. The TTAP used "accredited private sector evaluation laboratories."[60] Following the widespread unhappiness with the TCSEC and the evaluation process, representatives from NSA and NIST "joined with representatives from the governments of Canada, the United Kingdom, the Netherlands, France, and Germany to draft new international criteria." The resulting Common Criteria took the place of TCSEC during a transition period in 1999–2000.[61]

(U) In 1997 NSA's Information Security Directorate (INFOSEC) underwent a major reorganization into the Information Assurance Directorate (IAD). The name change was more than aesthetic. According to the first IAD director, Mike Jacobs, the changes addressed a new reality. The word "security" no longer fully described the needs of NSA's INFOSEC customers. Information technology was now complex and interconnected beyond the point of simply needing to be secure. Information assurance was an ever-changing combination of security, trusted data, and system availability. In this new environment, NSA had no claim to a monopoly on information security products and expertise. Partnering with industry was the only path to prosecuting the IA mission. Success was a matter of influence more than authority. No longer was NSA solely in the business of providing a COMSEC product that was years in the making and under their total control; now, they were also responsible for protecting computer data and the ever-expanding networks that housed it. NSA found itself in the business of reducing risks to commercial hardware and software components and systems that its personnel did not

design, build, or control any part of (including supply chains). As Jacobs said,

> . . . we were the monopoly, we had the best that money could buy, and we evaluated it to the point where we provided a virtual guarantee of security to the customer … and now we're confronted with … the realization that offering a guarantee today is virtually impossible … we don't have the capability, never will—and perhaps never should—to so thoroughly evaluate that technology that we could tell the same customer you have a virtual guarantee. That's just not going to happen.[62]

(U) IAD, Jacobs said, would instead be giving customers risk statements in the future, to allow them to manage their own risks. In the end, IAD and its personnel were able to build relationships with their customers and improve computer and system security.[63]

(U) Conclusion

(U) Information technology, in less than a generation, had brought about revolutionary changes in communications and in the way business was conducted within the government and throughout the world. The Department of Defense had led the way in inventing, deploying, and perfecting many of the technologies involved in the information revolution, with NSA offering critical expertise and insights throughout. The CSC and NCSC were a critical step in the Agency's changing relationship with information security. But the centers were not enough. DoD learned belatedly—though still faster than almost any other institution—that securing IT means far more than trusting computer hardware. Internally, the Agency's organizational structure had briefly left it unprepared for the scope and scale of the changes that new technology would bring. It was the Agency's involvement in the CSC that gave NSA the footing to adapt to the new, fast-changing reality of a crucial DoD-wide defensive mission.

Notes

1. (U) US Congress, "The Computer and Invasion of Privacy–Hearings before the Special Subcommittee on Invasion of Privacy, House Committee on Government Operations, 89th Cong., Second Session, July 26-28, 1966" (US Government Printing Office, 1966), 6, accessed May 27, 2022, https://books.google.com/books?id=LmAnLmmKJesC&pg=PA1&source=gbs_toc_r&cad=4#v=onepage&q&f=false. Horton's use of the word "computermen" is a reminder that computer science was still in its early stages and very new to the public in 1966. Less awkward terminology would follow in time.
2. (U) Rebecca S. Kraus, "Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants" (US Census Bureau, 2011), 1-6, 13-24, accessed May 27, 2022, https://www.census.gov/history/pdf/kraus-natdatacenter.pdf.
3. (U) Procurement of Automatic Data Processing Equipment, in Department of Defense Authorization Act, 1982, Pub. L. No. 97-86, December 1, 1981, accessed June 3, 2022, https://www.govinfo.gov/content/pkg/STATUTE-95/pdf/STATUTE-95-Pg1099.pdf#page=1.
4. (U) George F. Jelen, *Information Security: An Elusive Goal* (Harvard University, Center for Policy Research, 1985), II-68, accessed June 1, 2022, http://www.pirp.harvard.edu/pubs_pdf/jelen/jelen-p85-8.pdf.
5. (U) Willis Ware, "Security Controls for Computer Systems," *Defense Science Board Task Force Report on Computer Security* (RAND Corporation, 1970), v.
6. (U) Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 10.
7. (U) Ware, "Security Controls," vii.
8. (U) Eugene V. Epperly, "The Department of Defense Computer Security Initiative Program and Current and Future Computer Security Policies," in *Proceedings of the Second Seminar on the Department of Defense Computer Security Initiative Program* (National Bureau of Standards, 1980), J-4.
9. (U) US Department of Defense Directive (DoDD) 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems" (1972), 6, 9.
10. (U) [redacted] "Recollections: History of Computer Security at NSA" (unpublished manuscript, 1998), 25, Center for Cryptologic History, Ft. Meade, MD.
11. (U) Ware, "Security Controls," xv; James P. Anderson, "Computer Technology Planning Study" (US Air Force, 1972), 1, CCH Historian Projects File, USCC Collaboration NCSC and CSC Project.
12. (U) Jon Brodkin, "50 years ago, IBM created mainframe that helped send men to the Moon System/360 brought new era of compatibility, and its programs still run today," Ars Technica, April 7, 2014, accessed May 31, 2022, https://arstechnica.com/information-technology/2014/04/50-years-ago-ibm-created-mainframe-that-helped-bring-men-to-the-moon/.
13. (U) [redacted] "Recollections," 74-78.
14. (U) Anderson, "Computer Technology Planning Study."
15. (U) [redacted] "Recollections," 77-84.
16. (U) Lt Gen Lew Allen, memo to the Assistant Secretary of Defense (Comptroller), December 16, 1974, NSA Archives, Accession 43120, Document Reference ID A479485.
17. (U) [redacted] "Recollections," 88.
18. (U) David Cooke, memo to Director NSA, February 25, 1976, NSA Archives, Accession 32128, Document Reference ID A2798394.
19. (U) Thomas R. Johnson, *American Cryptology During the Cold War, 1945-1989: Book III: Retrenchment and Reform, 1972-1980* (Fort Meade, MD: Center for Cryptologic History, 1998), 144.
20. (U) Presidential Directive-24 (PD-24), "Telecommunications Protection Policy," 1977.
21. (U) Jelen, *Information Security,* II-65.
22. (U) Jelen, *Information Security*, II-62.
23. (U) As Walker would say later in an oral history interview, "trusted" was a carefully selected word. To suggest that a computer system was not "secure" raised alarms with government auditors. A computer was "secure" when it was locked in a vault. It was "trusted" when it could be used with confidence that it would protect information from unauthorized access. In reality, protecting data in an electronic system continues to be a combination of physical, administrative, hardware, and software

mitigations. Stephen Walker, "Oral history interview with Stephen Walker," interview by Jeffrey R. Yost, Charles Babbage Institute, November 8, 2012, retrieved from the University of Minnesota Digital Conservancy, accessed June 1, 2022, https://hdl.handle.net/11299/144021.

24. (U) National Institute of Standards and Technology, "National Computer Security Conferences (1979-2000)," accessed June 3, 2022, https://csrc.nist.rip/publications/history/nissc/index.html.
25. (U) Jelen, *Information Security*, II-78.
26. (U) Jelen, *Information Security*, II-80-83.
27. (U) The June 3, 1980, incident had occurred in the wee hours of the morning, when NORAD computers indicated a Soviet nuclear attack was underway. The warning got as far as then-National Security Advisor Zbigniew Brzezinski before the computer glitch was confirmed and the alert pilots were recalled. Doug Mataconis, "Dr. Brzezinski's 3 a.m. Phone Call," *Outside the Beltway*, May 27, 2017, accessed June 1, 2022, https://www.outsidethebeltway.com/dr-brzezinskis-300-am-phone-call/. The incident also helped inspire the 1981 movie *WarGames*. After the scriptwriters watched Walter Cronkite's reporting on the NORAD computer glitch, they were reassured that their scenario actually was plausible. John Badham (director), Lawrence Lasker (screenwriter), and Walter F. Parkes (screenwriter), "Audio commentary," *WarGames* (1983; MGM/UA, 2008), DVD.
28. (U) Jelen, *Information Security,* II-80–II-82.
29. (U) Jelen, *Information Security*, II-78, II-80–II-82.
30. (U) Jelen, *Information Security*, II-82–II-84.
31. (U) Jelen, *Information Security*, V-10.
32. (U) Jelen, *Information Security*, II-84–II-86.
33. (U) Jelen, *Information Security,* II-86–II-88; "A Guide to Understanding Audit in Trusted Systems," National Computer Security Center via National Institute of Standards and Technology CSRC, July 28, 1987, accessed June 1, 2022, https://irp.fas.org/nsa/rainbow/tg001.htm.
34. (U) Stephen Walker began the DoD Computer Security Initiative in 1978 while he was with the OSD C3I. Walker, interview.
35. (U) Anderson, "Computer Technology Planning Study," 32.
36. (U) US DoDD 5215.1, "Computer Security Evaluation Center," (October 25, 1982).
37. (U) Steven B. Lipner, "The Birth and Death of the Orange Book," in *IEEE Annals of the History of Computing* 37, no. 2 (April–June 2015): 23–25.
38. (U) "Trusted Computer System Evaluation Criteria," National Computer Security Center, December 26, 1986, accessed June 1, 2022, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf.
39. (U) Lipner, "The Birth and Death of the Orange Book," 24.
40. (U) The White House, "National Policy on Telecommunications and Automated Information Systems Security" (NSDD-145), September 17, 1984, accessed June 5, 2022, https://irp.fas.org/offdocs/nsdd/nsdd-145.pdf.
41. (U) White House, NSDD-145.
42. (U) NCSC, "Guide to Understanding Audit in Trusted Systems."
43. (U) NCSC, "Guide to Understanding Audit in Trusted Systems"; Warner Amendment systems refers to the 1981 Warner Amendment to the Brooks Automatic Data Processing Act of 1965. Senator John Warner (R-VA) sponsored the amendment, which was sub-titled "Law inapplicable to the procurement of automatic data processing equipment and services for certain defense purposes." This legislation amended the Brooks Act of 1965, by exempting DoD agencies from General Services Administration (GSA) oversight when the ADP requirement is for intelligence activities, national security, military command and control, or weapons systems. Computer Security Act of 1987, Pub. L. No. 100-235, January 8, 1988 [contains what is known as the Warner Amendment of 1988], accessed June 3, 2022, https://www.govinfo.gov/content/pkg/STATUTE-101/pdf/STATUTE-101-Pg1724.pdf.
44. (U) US Department of Defense Instruction (DoDI) 5215.2, "Computer Security Technical Vulnerability Reporting Program (CSTVRP)" (September 2, 1986).
45. (U) Representative Jack Brooks, statement before the Subcommittee on Transportation, Aviation,

and Materials, House Committee on Science and Technology, June 27, 1985.

46. (U) White House, NSDD-145.
47. (U) Representative Jack Brooks, statement before the Subcommittee on Legislation and National Security, House Committee on Government Operations, February 25, 1987.
48. (U) The Computer Security Act of 1987 carried over the language from Senator Warner's amendment from 1981. The CSA again amended the Brooks Act, this time by adding a waiver process for federal computer systems to the standards and guidelines that were to be developed by the National Bureau of Standards. During discussion of the Computer Security Act (then of 1986) in the House of Representatives on August 12, 1986, Representative Brooks—speaking in opposition to DoD's role in civilian computer security—noted, "I will be delighted to state again that this does not expand the Brooks Act. It does not expand the authority of the GSA. The Defense Department will still be operating under the Warner provisions. Everything that moves, shakes, flies, digs, shoots, crawls, hops, skips, that has a computer in it that the Defense Department has got the money for and has built is all exempted now, has been and will be." 100 Cong. Rec. R21023 (1986), accessed June 2, 2022, https://www.congress.gov/99/crecb/1986/08/12/GPO-CRECB-1986-pt15-1-2.pdf.
49. (U) National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: The National Academies Press, 1991), 195; *PC Magazine,* "NCSC," accessed May 31, 2022, https://www.pcmag.com/encyclopedia/term/ncsc.
50. (U) Computer Security Act of 1987.
51. (U) The White House, "National Policy for the Security of National Security Telecommunications and Information Systems" (NSD-42), July 5, 1990, accessed June 3, 2022, https://irp.fas.org/offdocs/nsd/nsd42.pdf.
52. (U) National Research Council, *Computers at Risk,* 195.
53. (U) *PC Magazine,* "NCSC"; Computer Systems Laboratory Bulletin, "Computer Security Roles of NIST and NSA," February 1991, accessed June 2, 2022, https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/csl-bul1991-02.txt.
54. (U) Paperwork Reduction Act of 1995, Pub. L. No. 104-13, May 22, 1995, accessed June 3, 2022, https://www.govinfo.gov/content/pkg/PLAW-104publ13/html/PLAW-104publ13.htm.
55. (U) Information Technology Management Reform Act of 1996/Federal Acquisition Reform Act of 1996/Clinger-Cohen Act of 1996, Pub. L. No. 104-106, February 10, 1996, accessed June 3, 2022, https://www.govinfo.gov/content/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf.
56. (U) National Computer Security Conferences (1979-2000), National Institute of Standards and Technology, accessed June 3, 2022, https://csrc.nist.rip/publications/history/nissc/index.html; Cliff Stoll, *Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989).
57. (U) Eliot Marshall, "Computer Security: NAS Sounds the Alarm," *Science* 250, no. 4986 (December 7, 1990): 1330, accessed June 2, 2022, https://www.science.org/doi/pdf/10.1126/science.250.4986.1330.
58. (U) *PC Magazine,* "NCSC."
59. (U) Lipner, "The Birth and Death of the Orange Book," 29; NSTISSAM COMPUSEC/1–99 March 11, 1999, "Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation," CCH Historian Projects File, USCC Collaboration NCSC and CSC Project.
60. (U) NSTISSAM COMPUSEC/1-99 March 11, 1999, "Advisory Memorandum."
61. (U) NSTISSAM COMPUSEC/1-99 March 11, 1999, "Advisory Memorandum"; Neal Thompson, "NSA, counterparts sign pact on securing computer networks–agreement sets standards for protecting software, systems from intruders," *Baltimore Sun*, October 6, 1998, accessed June 1, 2022, https://www.baltimoresun.com/news/bs-xpm-1998-10-06-1998279080-story.html.
62. (U) Michael Jacobs, interview by Jimmy Collins and David Hatch, April 16, 2002 and May 16,

2002, NSA–OH–2002–10, transcript, Center for Cryptologic History, Ft. Meade, MD.
63. (U) Jacobs, interview, 15-16.

(U) Classification Source

(U) NSA/CSS Classification Guide 6-1, Classification Guide for NSA/CSS Information Systems 6-1, E.5.

(U//FOUO) **Evan Rea** joined the Center for Cryptologic History in March 2021. A historian by training and a facilities project manager by trade, he spent his first 10 years at NSA in the Office of Installations and Logistics (I&L). While in I&L, he worked as a project manager and section chief in the extended enterprise, planning and managing new construction and renovation projects at NSA field sites around the world.

(U//FOUO) **Kara Smit** joined US Cyber Command's History Office in August 2019. A former US Navy calibration technician and linguist, she has more than 30 years combined service in the US Navy and Intelligence Community. As a contractor, she has worked as a linguist, an office manager, and in the Air Force Cryptologic Office in the Business Management Directorate and the Compliance, Policy, and Oversight Division.