

**SUMMARY OF THE
REPORT OF THE JUDICIAL CONFERENCE COMMITTEE
ON AUTOMATION AND TECHNOLOGY**

The Committee on Automation and Technology recommends that the Judicial Conference:

- In 2002, a review of system architecture will be completed under the committee's direction, with a view of possible decentralization of Internet access to individual courts in a manner consistent with the security of the entire judiciary network. Pending the completion of this review, we ask the Judicial Conference to reaffirm (a) that computers connected to the DCN shall access the Internet only through national Internet gateways; and (b) that operations and security at those gateways are under the administrative, managerial, and logistical control of the Administrative Office, subject to the direction of the Conference or, where appropriate, Conference committees. pp. Addendum 2-7
- Immediately adopt, on an interim basis, the model use policy at Appendix D developed by the federal Chief Information Officers Council, as later revised by the subcommittee or the committee to tailor it to the judiciary, as a national minimum standard defining appropriate Internet use, subject to the right of each court unit to impose or maintain more restrictive policies. In carrying out routine administrative, operational, and maintenance responsibilities, should instances of possibly inappropriate use of government resources come to the attention of the management of a court unit or the Administrative Office, established Judicial Conference notification policy will be followed.. . . . pp. Addendum 7-10
- Reaffirm that individual courts have responsibility to enforce appropriate use policies and direct that the Administrative Office, as part of its regular audit process, examine and comment upon the adequacy of the courts' enforcement methods.. . . . pp. Addendum 10

NOTICE
NO RECOMMENDATION PRESENTED HEREIN REPRESENTS THE POLICY OF THE JUDICIAL

- Require the Administrative Office to disseminate to all judicial branch employees now and hereafter hired, and to request each court prominently to display on screen prior to access of the DCN and the Internet, a banner notice clearly and conspicuously disclosing, in such form as the subcommittee or the committee may approve, that the use of the system is subject to the interim policy or, where applicable, more restrictive local policy, that the contents of the use may be viewed and recorded, that the employee's use of the system constitutes consent to such viewing and recording, and that uses inconsistent with the applicable use policy may result in disciplinary action. pp. Addendum 10-11
- Having discerned no material business use for Gnutella, Napster, Glacier, and Quake, all of which raise immediate and continuing security vulnerabilities, direct the Administrative Office to take appropriate steps to block such traffic involving computers connected to the DCN, and (2) delegate to the committee the authority to block other tunneling protocol that may cause security breaches. pp. Addendum 13-14

The remainder of the report is submitted for the record.

**Agenda F-3 (Addendum)
Automation and Technology
September 2001**

**ADDENDUM TO THE
REPORT OF THE JUDICIAL CONFERENCE COMMITTEE
ON AUTOMATION AND TECHNOLOGY**

The Judicial Conference Committee on Automation and Technology (committee) met in a special session on July 27, 2001, to address matters related to information technology security and Internet use. All members were present with the exception of Judge L. T. Senter, Jr., who was unavoidably absent. Also attending the meeting were Administrative Office personnel Clarence A. Lee, Jr. (Associate Director for Management and Operations); Melvin J. Bryson (Assistant Director for Information Technology); Barbara C. Macken (Deputy Assistant Director for Information Technology/Chief Operating Officer); Richard D. Fennell (Chief Technology Officer); Terry A. Cain (Chief, Information Technology Policy Staff); Craig W. Jenkins (Chief, Infrastructure Management Division); and Neal Dillard (Infrastructure Management Division).

On July 24, 2001, the committee's Subcommittee on IT Architecture and Infrastructure, which had been charged with reviewing these matters, met by teleconference and developed a number of recommendations which were acted upon by the committee. This addendum to the committee's September 2001 report contains background information as well as the full committee's recommendations regarding operations of the national communications infrastructure, appropriate use, noticing of judiciary employees, and protecting the judiciary's communications infrastructure.

Judiciary's National Communications Infrastructure

Background

The judiciary's data communications network (DCN) was established to provide a dedicated, separate, and secure infrastructure for the transmission of data and electronic communications among the 800 building sites within the federal judiciary. Begun in 1991 and completed in 1998, the DCN provides judges and court staff a secure capability to send electronic mail, to access judiciary computer systems, and to transfer data. The DCN is the combined judiciary network consisting of centrally managed wide-area networks (routers and leased communications services that connect judiciary facilities nationwide) and local-area networks (servers, desktop computers, routers, and telecommunications equipment installed in and maintained by local courts). It is currently comprised of the private network used by judiciary employees and the public access network (also known as PacerNet) used by the general public to access electronic public access applications, such as the new case management/electronic case filing systems, and court-based web sites.

During the mid-1990s, as the Internet's world-wide web began to emerge as a means of global communications, information-sharing, and business transaction, providing judiciary employees with access to the Internet became desirable. Some courts and employees began to install Internet connections on their own, unmindful of the potential risks to the security of the DCN and the judiciary's sensitive information. The Internet is not a secure communications channel, and its use by individuals connected to the DCN posed substantial risk of intrusions by hackers and other unauthorized users. To protect the integrity of the judiciary's secured network from the risks inherent to the unsecured public

Internet, the judiciary needed to put into place a means for appropriately controlled access to the Internet.

On recommendation of the committee, in September 1997 the Judicial Conference approved a judiciary-wide policy aimed at protecting the security of the judiciary's electronic systems and information. The policy requires that, for computers connected to the DCN, access to the Internet may be provided only through national gateway connections approved by the Administrative Office pursuant to procedures adopted by the Committee on Automation and Technology.¹ Accordingly, national gateways have been established at the Administrative Office, the Fifth Circuit, and the Ninth Circuit. Each gateway serves multiple circuits.

In June 1998, the committee discussed preparation of a security configuration for all national gateways that would establish minimum security standards.² Underlying the security plan was the need to maintain a rigorous security environment to which all national gateways would be subject equally and which provides for regular security audits to uncover any weaknesses. An independent, recognized leader in risk analysis and security planning assisted with creating a standard security architecture for the gateways and recommended a number of security control measures, including intrusion detection software. These recommendations, provided to and commented on by representatives from each of the national gateways, helped define the security apparatus employed at the gateways.

¹JCUS-SEP 97, pp. 52-53.

²Although the plan was not scheduled to be completed until the end of that summer, at its June 1998 meeting, the committee requested that certain aspects anticipated to be a part of the security plan, specifically 24-hour Internet access monitoring at the gateways, be implemented immediately (AUTTECH-SEP 98, pp. 6-7). The term "monitoring" suggests a far more active and penetrating level of scrutiny than actually occurs in the judiciary. The judiciary's practices in this regard generally consist of nothing more than logging any Internet contacts that meet predefined security-based criteria.

By late 1999, the security architecture, using complementary technologies (firewalls and intrusion detection software) to protect the judiciary's networks and to mitigate risks, was in place. A firewall enforces general predefined entry and exit rules for an entire network, but it is not designed to identify and counter attack patterns. Intrusion detection software complements the firewall by monitoring network and server activity for signs of malicious intent, such as denial of service attacks, unauthorized access attempts, and pre-attack reconnaissance probes. When this software detects such activities, the system can respond in a number of ways: recording the event, notifying the network administrator, or terminating the attack.³ The National Security Agency recognizes firewalls and intrusion detection software as integral components of an enterprise-wide security threat management system.

The annual telecommunications cost for the current leased-line wide-area network is approximately \$10 million, excluding hardware and personnel. Additionally, the annual budget for the national gateways supporting browser and e-mail Internet access for the judiciary is approximately \$1.2 million. Internet use accounts for more than 75 percent of the total traffic across the DCN. The remaining 25 percent of traffic is for internal e-mail, non-Internet-based computer-assisted legal research, and other judiciary applications including case management and administrative systems. Thus, the current estimated cost for providing Internet services across the DCN is more than \$8.4 million annually and is rising.

³An analogy would be to think of the network as a high-rise apartment building, with the firewall as the doorman, and each intrusion detection system sensor as a guard dog on a specific floor. The doorman is generally quite good about letting the right people in and keeping the wrong people out. However, a moderately clever criminal will be able to get past the doorman and into the building. The guard dog is better at knowing who is authorized to be on the floor and responding quickly to stop the intrusion.

In December 2000, the committee was informed of efforts to develop a comprehensive information technology security plan for the judiciary. Also at its December 2000 meeting, the Committee on Automation and Technology requested the Administrative Office to analyze the explosive growth in Internet browser and e-mail traffic. To conduct this analysis, the Administrative Office employed the capabilities of the intrusion detection software – a primary component of the overall security scheme for the judiciary’s data communications and public access networks – which is installed at each of the national gateways. The analysis revealed that a significant factor contributing to the growth of this traffic appeared to be related to personal, rather than business usage.

The committee’s security efforts were endorsed by the Executive Committee in March 2001, which identified specific concerns for inclusion. The Executive Committee also discussed matters related to the use of the Internet and information technology security at its meetings and teleconferences held in March, May, and June 2001, and requested the Committee on Automation and Technology, on an expedited basis, “to develop policies and procedures to protect the confidentiality of electronic judicial communications and work product, including appropriate controls on monitoring such communications and work product.”⁴

On May 24, 2001, the Ninth Circuit Judicial Council directed its staff to disable the intrusion detection software at the national gateway located in San Francisco. That action gave rise to concerns for the security of systems and information on all the judiciary’s computer networks, particularly in the Eighth, Ninth, and Tenth Circuits, whose systems are served by that gateway. In order to secure reactivation of the intrusion detection software, the Executive

⁴These requests are documented in memoranda of action dated March 12, May 24/31, and June 19, 2001.

Committee asked the Administrative Office to remove detection signatures that had theretofore permitted the detection and logging of transfers of large music and movie files. The software was reactivated without the music and movie signatures, on June 4, 2001, and the intrusion detection software sensors were modified accordingly at all gateways.

Operation of the National Gateways

The Director of the Administrative Office of the United States Courts is the chief administrative officer for the federal courts as defined in 28 U.S.C. § 604. Among his duties, the Director shall “supervise all administrative matters relating to the offices of the clerks and other clerical and administrative personnel of the courts”⁵ and “audit vouchers and accounts of the courts.”⁶ These sections of title 28 parallel the statutory requirements levied upon executive branch agency heads and therefore require the Director to establish internal accounting and administrative controls that reasonably ensure that all assets are safeguarded against waste, loss, unauthorized use, and misappropriation. Section 604 provides that the Director carries out his responsibilities under the supervision and direction of the Judicial Conference of the United States.

In the legislation that authorizes the Judiciary Information Technology Fund (28 U.S.C. § 612), the Director is to “establish effective Administrative Office oversight of court automation efforts to ensure the effective operation of existing systems and control over developments of

⁵28 U.S.C. § 604(a)(1).

⁶28 U.S.C. § 604(a)(11).

future systems,” and to “assess the current utilization and future user requirements of the data communications network.”⁷

At this meeting, the committee discussed how some aspects of the information technology program – notably office automation and local-area networks – have been decentralized to the courts.⁸

As part of the national communications infrastructure, however, the national gateways have been funded, operated, maintained, and supported by the Administrative Office, primarily because of the need to maintain a consistent security posture and also because of the potential workload on the courts.

The committee agreed this is the appropriate model for the time being.

Recommendation: In 2002, a review of system architecture will be completed under the committee’s direction, with a view of possible decentralization of Internet access to individual courts in a manner consistent with the security of the entire judiciary network. Pending the completion of this review, we ask the Judicial Conference to reaffirm (a) that computers connected to the DCN shall access the Internet only through national Internet gateways; and (b) that operations and security at those gateways are under the administrative, managerial, and logistical control of the Administrative Office, subject to the direction of the Conference or, where appropriate, Conference committees.

Appropriate Use of Government Resources

The judiciary is accountable both to Congress and to the public for the manner in which it expends funds and manages its resources. Under 31 U.S.C. § 1301, “appropriations shall be applied only to the objects for which the appropriations were made, except as otherwise provided by the law.”

⁷Other statutes also bear on the Director’s responsibility for the management of information technology resources in the federal judiciary. For example, the Computer Security Act of 1987 applies to the judiciary and requires adherence to guidelines and standards for ensuring the “cost-effective security” of sensitive information in federal computer systems, the primary purpose of which is to “control” the “loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse.”

⁸Authorized in 28 U.S.C. § 5602(a), decentralization allows each court to operate with considerable autonomy in accordance with policies and guidelines set at the national level.

In applying this statute, it is axiomatic that federal monies are to be expended to further the agency's mission-related purposes. Employees who use government resources excessively for personal use are potentially subject to criminal prosecution under 18 U.S.C.

§ 641. Similarly, the Computer Fraud Abuse Act, 18 U.S.C. § 1030, provides for criminal penalties for unauthorized use or "use exceeding authorization" of a federal government computer under certain circumstances, including where the individual obtains anything of value (defined as exceeding \$5,000).

The judiciary has embraced these concepts. For example, the Code of Conduct for United States Judges and the Code of Conduct for Judicial Employees state that all persons employed by the judiciary "should respect and comply with the law and should act at all times in a manner that promotes public confidence in the integrity and impartiality of the judiciary." Moreover, the Committee on the Budget, at its July 19-20, 2001, meeting, resolved that it is incumbent on the judiciary to ensure that it employs adequate safeguards over the use of its property and resources and asked this committee to "take steps to ensure that judiciary automation property and facilities are used for official purposes."⁹

Appropriate use policies for government resources are generally established to define the responsibilities and privileges that employees must observe in their use of institutionally provided resources. These policies also set forth the roles and responsibilities of managers to develop, maintain, and disseminate the policies, as well as assign responsibilities and procedures for addressing inappropriate use. The establishment of and compliance with appropriate use policies should limit the organization and its employees from potential exposure to legal liabilities, misdirection of resources, and institutional embarrassment.

⁹See Agenda F-5, pp. 9-10.

In 1997, the Judicial Conference urged all courts to adopt local policies that would establish local responsibility for managing employee access to the Internet and that would provide guidance on the responsible use of the Internet. Each policy should contain, at a minimum, a definition of what constitutes “acceptable or responsible use” of the Internet.¹⁰ Since then, the Administrative Office has sent periodic memoranda and other materials providing guidance to the courts, and some courts have since adopted policies.

At this meeting, the committee examined how other government agencies have addressed the use of the Internet and discussed a potential national appropriate use policy for the judiciary. In 1999, the General Services Administration distributed to all executive branch agencies a recommended model policy and guidance on appropriate use of government equipment. The model policy was developed by the Federal Chief Information Officers Council in conjunction with various government ethics, legal, procurement, and human resource experts. The committee was informed that, according to the General Services Administration, approximately two-thirds of the executive branch agencies have adopted or adapted this model policy. The remaining agencies, for the most part, have established more restrictive policies, primarily due to network capacity limitations. With respect to the legislative branch, this model policy has been approved by congressional leadership. This model policy is contained in Appendix D.

The committee unanimously agreed on the importance of a national appropriate use policy as a minimum standard to which all courts should adhere. The committee found that the proposed model policy, already in use by most of the federal government, was reasonable and would promote public confidence that the judiciary’s resources are well managed, and its assets are used appropriately. The committee therefore recommends that the Judicial Conference immediately adopt, on an interim basis,

¹⁰JCUS-SEP 97, pp. 52-53.

the model policy used by most of the federal government. The committee will tailor the model policy to the judiciary and will propose a permanent policy at the Judicial Conference's March 2002 session.

Recommendation: That the Judicial Conference immediately adopt, on an interim basis, the model use policy at Appendix D developed by the federal Chief Information Officers Council, as later revised by the subcommittee or the committee to tailor it to the judiciary, as a national minimum standard defining appropriate Internet use, subject to the right of each court unit to impose or maintain more restrictive policies. In carrying out routine administrative, operational, and maintenance responsibilities, should instances of possibly inappropriate use of government resources come to the attention of the management of a court unit or the Administrative Office, established Judicial Conference notification policy will be followed.

This national policy is intended to complement local policies by establishing a minimum standard. As noted above, the Judicial Conference has previously urged courts to adopt local policies establishing local responsibility for managing employee access to the Internet and providing guidance on the responsible use of the Internet. At this meeting, the committee agreed to ask the Judicial Conference to clarify that courts are also responsible for enforcing their local use policies. Having noted that the Administrative Office performs cyclical financial audits to measure, among other elements, compliance with applicable policies and procedures, the committee also requests the Judicial Conference to ask the Administrative Office to examine and comment upon the adequacy of the local courts' enforcement methods as a matter of course in these cyclical audits.

Recommendation: That the Judicial Conference reaffirm that individual courts have responsibility to enforce appropriate use policies and direct that the Administrative Office, as part of its regular audit process, examine and comment upon the adequacy of the courts' enforcement methods.

To assist the courts in their enforcement of local policies, the Administrative Office will make software and other tools available to the courts for their use.

Notice to Judiciary Employees

Some questions have been raised as to whether adequate notice had been provided to judges and court staff that systems activity logs were being monitored. The committee noted that since 1995, the Administrative Office has issued guidance to the courts about the importance of affirmatively alerting all users that their Internet usage is subject to monitoring, but that courts have not followed this advice consistently. To guarantee beyond doubt that adequate notice will have been given and assuming the Judicial Conference acts favorably on the committee's recommendations regarding a national appropriate use policy, the committee recommends the following:

Recommendation: That Judicial Conference require the Administrative Office to disseminate to all judicial branch employees now and hereafter hired, and to request each court prominently to display on screen prior to access of the DCN and the Internet, a banner notice clearly and conspicuously disclosing, in such form as the subcommittee or the committee may approve, that the use of the system is subject to the interim policy or, where applicable, more restrictive local policy, that the contents of the use may be viewed and recorded, that the employee's use of the system constitutes consent to such viewing and recording, and that uses inconsistent with the applicable use policy may result in disciplinary action.

Protecting the Judiciary's Communications Infrastructure

Procedures for Enabling "Signatures"

The intrusion detection software sensors installed at the national gateways function by detecting predetermined patterns, or "signatures," indicating potentially malicious activities as traffic passes through the national gateways. As noted above, since June 4, 2001, the intrusion detection software installed gateways has operated without two specific signatures that allow identification of high-volume music and movie files activated, pending development of policies and procedures. After lengthy discussion at this meeting, the committee acknowledged the dynamic nature of information technology necessitated an ability to respond quickly to threats. Use of the intrusion detection software at the national gateways has provided the judiciary with tangible findings of unauthorized external access to

the judiciary's public access network not prevented by the firewall. The intrusion detection software logs can also provide forensic data that is essential to the successful apprehension of hackers.¹¹ The committee recognizes that a more formal mechanism of enabling additional signatures to detect, evaluate, and respond to unauthorized network and system access attempts would be desirable.

C Pending a report by the committee by December 2001 on Internet security and appropriate Internet use, no intrusion detection software signatures that were not active as of July 24, 2001, will be activated without the committee's approval, provided, however, that the Administrative Office may activate additional signatures, for security purposes only, prior to obtaining approval by the committee in order to respond to security threats. In the event the Administrative Office activates additional signatures for security purposes, the additional signature(s) shall be deactivated not more than 14 calendar days later absent an extension granted by the committee chair or any member of the committee designated by the chair, pending review by the committee. Where it concludes that further input would be beneficial, the committee will require reasonable dissemination within the judiciary community of such requests to gain the benefit of additional views on the security concerns and the appropriate means of addressing them. Further, the Administrative Office shall promptly notify the committee chair or his designee upon making any other changes to its security measures. Nothing herein, however, restricts the Administrative Office's ability to update existing signatures and implement patches provided in the normal course by the intrusion detection software provider.

Specific Concerns with "Tunnels"

Several Internet programs are designed to bypass firewalls and create direct peer-to-peer (computer-to-computer) connections known as tunnels. The intrusion detection software is set to detect and record such traffic. Tunnels are created when judiciary users, either knowingly or unknowingly, make use of products or programs that establish a connection with a computer outside the firewall through a tunnel. Not only do they expose the judiciary to viruses and other software

¹¹For example, at the request of the Federal Bureau of Investigation, the judiciary built an intrusion detection software signature to track and document the activities of a hacker who is alleged to have caused approximately \$1.5 million in lost PACER revenue. The same signature subsequently detected other suspicious activity which led to the discovery of the on-line theft of judiciary password files by a contract employee

vulnerabilities, but tunnels also weaken the security of the DCN because these sessions can be used by a hostile external party trying to connect to judiciary systems. Tunnels can be used for large data transfers that impact the performance of concurrent legitimate business activities being conducted over the DCN. Programs with a legitimate business use generally would not need to bypass an organization's security apparatus.

Examples of programs that create tunnels include some information search and transfer services (for example, "Gnutella" and "Napster") which bypass security safeguards and open the judiciary to malicious features hidden in the files; "back door programs" (such as "Glacier") that allow intruders to gain remote control of a desktop computer or server operating system without the knowledge or consent of an authorized user, allowing outsiders to view the computer's screen, record passwords, obtain system information, manipulate files, or even shut down the computer; and games (for example, "Quake"), whose tunnels created from a DCN user's desktop permit an unauthorized external user access to a judiciary computer during a game session.

In March 1999, the Judicial Conference declined to authorize the national gateways to employ filtering software to block access to adult-oriented, pornographic web sites on the Internet. The Judicial Conference, viewing this as a local matter, declined to approve the recommendation.¹² Since then, the filtering software has been available to any court on request so that it could activate it in accordance with local policy.

The current situation, however, is vastly different, in that the tunnels created by these programs jeopardize the security of the DCN and, as a result, may threaten judiciary data. The intrusion detection software, which is designed primarily for security and not as a filtering mechanism, has a

¹²JCUS-MAR 99, pp. 8-9.

feature whereby certain signatures can be defined and the sensors configured to terminate or prevent connections to sites that match these signatures. The committee makes the following recommendation:

Recommendation: That the Judicial Conference, (1) having discerned no material business use for Gnutella, Napster, Glacier, and Quake, all of which raise immediate and continuing security vulnerabilities, direct the Administrative Office to take appropriate steps to block such traffic involving computers connected to the DCN, and (2) delegate to the committee the authority to block other tunneling protocol that may cause security breaches.

Security Study

At its June meeting, the committee was informed of efforts to develop a security plan. At this meeting, the committee took the following action:

- C The committee requested that an independent security study covering those aspects of the judiciary's information technology program under the jurisdiction of the Judicial Conference and the Director be conducted, using appropriate independent consultants reporting to the committee, and completed in sufficient time to permit action in December 2001.



Edwin L.

Nelson, Chair
David A. Baker
Paul J. Barbadoro
Alice M. Batchelder
David H. Coar
David A. Faber
Lewis A. Kaplan
John Thomas Marten
Richard L. Nygaard
Catherine D. Perry
James Robertson
L. T. Senter, Jr.
Diane W. Sigmund
Roger G. Strand

August 13, 2001