U. S. Department of Justice
Information Technology Strategic Plan

Appendix D

Department of Justice Telecommunications Strategy

White Paper

Appendix D
Telecommunications Strategy White Paper*

Telecommunications at the DOJ comprises data networks, conventional voice networks, and wireless networks that include cell phones, radios, and data devices such as Personal Digital Assistants. This material focuses primarily on the strategy for the DOJ's data networks.

Background

Almost all of the DOJ's data networks are based on the TCP/IP protocol family. These IP networks are implemented using a variety of technologies that include leased lines, Asynchronous Transfer Mode (ATM), and Frame Relay circuits. There are a few exceptions to this rule, e.g., video conferencing services, and these exceptions are evolving to IP networks. Generally, these specialty service networks have been developed and operated by DOJ components.

The DOJ IP network is a "network of networks" Viewed from an IP-perspective, the DOJ network comprises a number of independent, national networks developed and operated by each of the major DOJ components. These individual networks are generally hierarchically organized, reflecting the organization structure of a DOJ component, as illustrated in Figure 1. The heavier lines in this figure are wide-area network connections (discussed later in this section). Each office building has a local area network. Each DOJ component network has a headquarters site that acts as the communications hub for that DOJ component. Interconnections between DOJ components are typically done between headquarters sites (usually in metropolitan Washington, DC), via the Justice Management Division (JMD) network. Connections with other outside entities, including other Federal agencies and the JMD-provided services (such as Internet access and an e-mail gateway), are typically performed through a DOJ component's headquarters site as well.

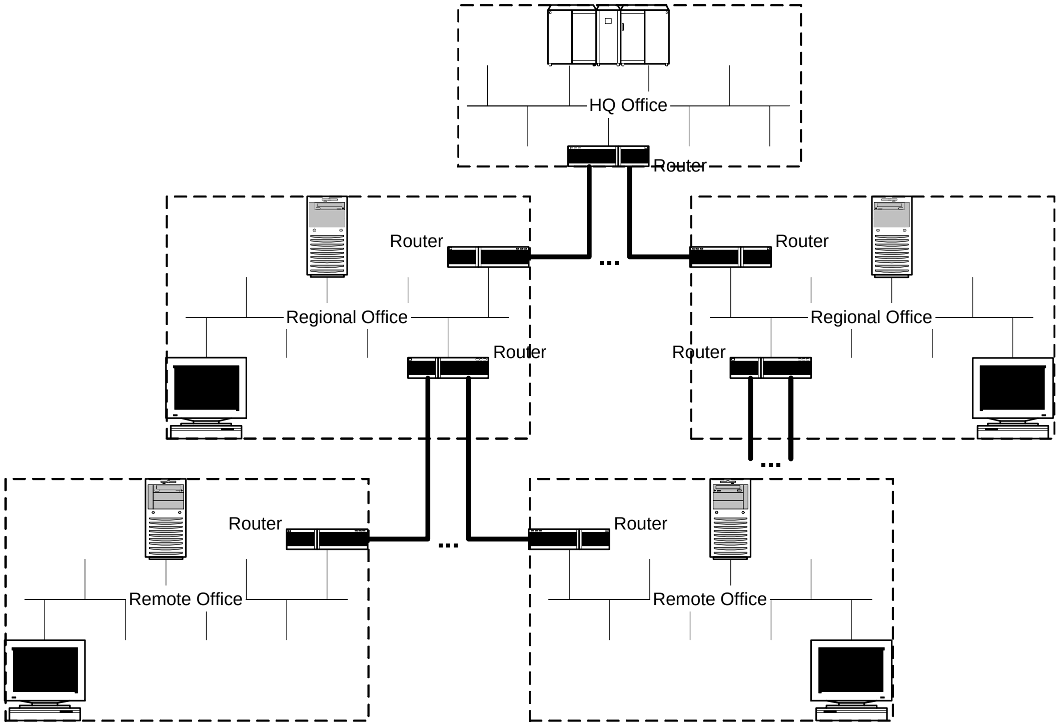

Figure 1

Typical Organization of a DOJ Component Network

* This White Paper is based on unpublished material prepared by the Rand Corporation for the Department of Justice.

The MAN or JMD network is not a national network, but primarily serves the Washington, DC area. It provides transit for traffic exchanged between DOJ component networks (horizontal sharing); common services such as an e-mail translation service, a gateway to the Internet, and external web servers; and provides access to shared data centers. These network relationships are illustrated in Figure 2.

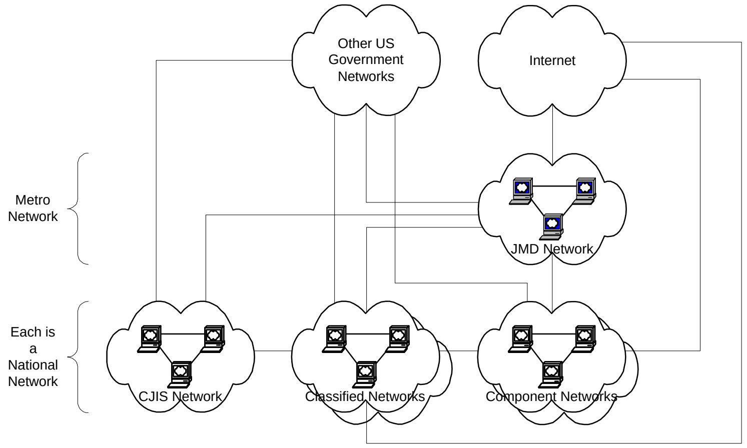

Figure 2

DOJ Networks and Their Relationships

Figure 2 represents the details of individual DOJ component networks as a communications "cloud". Each of the component networks (as well as some of the classified networks and CJIS) is national in scope and has an implementation similar to the network shown in Figure 1. Figure 2 suppresses many important details. For example, it does not show firewalls, gateways or specific hosts. It is intended to label the types of existing networks and shows a simplified view of the connectivity among them.

The DOJ component networks include unclassified networks, generally carrying Sensitive, But Unclassified (SBU) traffic; classified networks (such as those serving the FBI and DEA); and the network enabling vertical sharing of information with local and state law enforcement agencies – the Criminal Justice Information System (CJIS) network.

There is a DOJ-wide policy stating that the JMD is to provide the only Internet access for the DOJ as a whole, in order to assure a common policy governs security functions such as screening for viruses, and intrusion detection. In addition to dial-in access, the JMD is now piloting Virtual Private Network (VPN) functions that provide secure access to the DOJ's networks from home, hotels, and other remote locations with access to the public telephone network. In practice, there are additional direct connections to the Internet, other than that provided by the JMD (e.g., the connection maintained by the BOP). Many DOJ components maintain dial-up access to the Internet from individual machines, dedicated to this purpose. Some provide dial-in access from the Internet. The JMD also provides a dial-in access service to most DOJ networks. Each of these additional points of interconnection with the Internet or other external network is managed by a different DOJ component with a potentially different policy about security. Multiple policies weaken DOJ's overall security posture against external threats.

The DOJ's IP networks are built from a variety of public network technologies and services. The DOJ has been pursuing a strategy calling for *all* DOJ networks, including classified networks and CJIS, to be built using the Justice Consolidated Network (JCN). Conceptually, the JCN is a reseller of Sprint's national ATM backbone – a public network that carries non-DOJ, and non-US Government traffic. The JCN also provides value-added services: a network operations center, managed network services (e.g., configuration and operation of network elements used to construct a DOJ component's network), and customer premises equipment for traffic aggregation. About two-thirds of all of the DOJ's unclassified network locations are serviced by the JCN.

In late 2001, a decision was made to exempt the FBI's Trilogy project from using the JCN. The waiver allowed another supplier, MCI, to be used to expedite the FBI's network and Office Automation (OA) upgrade project. The FBI's network is a completely classified network. It has a strategy that calls for the development of a trusted guard that will connect it to the JMD network for the exclusive purpose of delivering unclassified e-mail.

The JCN was conceived to promote information sharing while minimizing total DOJ costs for data network services. The cost savings have been marginal. This was a consideration in the decision to rebuild the FBI's network using a second supplier. The information sharing objective has not been realized either. The DOJ operates multiple national networks, each serving a DOJ component. Sharing of an application between DOJ components (e.g., an application run by one component, and accessed by another) requires a customized connection between hosts residing in each component's network. Sharing of data between DOJ components is typically done by regularly extracting a copy of some subset of data "owned" by one DOJ component and providing that extract to another DOJ component under the terms of a Memorandum of Understanding (MOU) governing its use. Extracts are typically communicated as a file transfer between DOJ component networks or through some other media such as tape.

Vision

The DOJ Information Technology Strategy is based on a vision of a DOJ-wide, national network that enables data and application sharing. Such a network will continue to be based on the TCP/IP protocol family, since this is the dominant industry standard for all applications, operating systems platforms, and network equipment. A single, national IP network, rather than the current arrangement of multiple national IP networks is the best solution to achieve this critical Department objective.

A single, national IP network provides the foundation for implementing DOJ-wide policies that reduce barriers to information and application sharing among components while advancing overall security. This network should be a Department utility that serves *all* DOJ components. A single, Department network provides any-to-any communications between DOJ components. This is the critical first step in a DOJ-wide information-sharing infrastructure. The network should be accompanied by a security infrastructure that is discussed in another section of this report. The vision for a Department data network is illustrated in Figure 3.

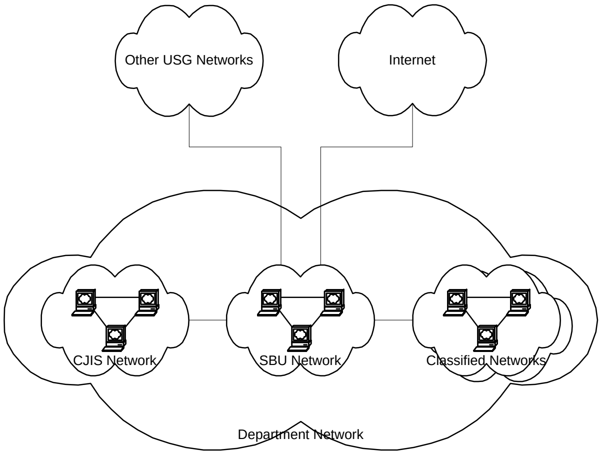

Figure 3

Vision

Every unclassified DOJ component network currently makes an independent decision on how to implement the transport of SBU traffic. Some DOJ components encrypt all traffic over public links; others do not encrypt SBU traffic over any links. A single, Department network for SBU traffic assures that there is a uniform policy for how SBU traffic will be carried. A Department policy, if based on encryption of traffic over public links, would improve security for the entire DOJ.

A Department network provides for clear accountability. One organization is accountable for end-to-end communications. This is a critical enabler for sharing of applications and data collections among DOJ components. Today, the goal of sharing an application or data can be defeated by conflicting priorities and commitments made by multiple DOJ component organizations that must make changes to their separate networks to enable sharing.

A critical element of any security strategy requires that interconnection of the DOJ's network to non-DOJ networks be carefully managed. The Department SBU network would define the perimeter for a DOJ-wide defense against external threats. DOJ must connect to the Internet, other US Government networks, State, Local, and Tribal data networks, and private networks in the public sector. The nature of these interconnections includes direct access, dial-up access, and virtual private networks. A uniform policy governing firewalls, virus scanning, and intrusion detection can be implemented at these points of interconnection. A Department network can minimize the number of interconnections to external networks. It can eliminate duplicative

efforts to monitor such interconnections. It can reconcile conflicting policies governing how multiple interconnections are operated (e.g., what viruses scans are performed).
Data networks are fundamental to the DOJ's daily operations and the execution of its mission. Interruptions of data connectivity must be managed in terms of frequency, duration of outage, and effort required to recover from the interruption. A Department data network can eliminate duplicate network contingency planning efforts in DOJ components, and promote effective and efficient network contingency planning DOJ-wide.

Every data network must be managed. A wide-area network supplier who already provides high-quality network management for its network should be selected to provide and manage the DOJ network. Such suppliers also provide managed network services for network equipment on customer premises. Currently, many DOJ components staff a network management center for their national network, and these, in turn, are further duplicated by the JCN network management center. A supplier-managed, Department network can eliminate the duplicate network management functions that are performed today by DOJ components and the JCN. Service level agreements should be employed to assure that the supplier's network management services meet *all* DOJ needs. Properly managed, a Department network would let DOJ components streamline their help-desk operations to focus on their information systems.

It is also important for DOJ employees to be able to access their networks, applications, and data stores when away from their desktops. Future demands for remote access will go beyond dial-up. They will also require access from offsite work locations, travel locations (e.g., hotels and airports), meeting sites, courtrooms, residences, and, indeed, wherever an employee happens to be when he or she needs to get work done. Wireless Ethernet (802.11b) hotspots are but the latest such opportunity for remote access.[1] Wireless access may range from broadband (e.g., from suitably-equipped homes, work sites, and hotels) to more restricted wireless connections. Indeed, remote access links ought to be able to support high-bandwidth big-screen clients as readily as low-bandwidth small-screen (e.g., PDA) clients. They also ought to be broadly compatible with commercial services regardless of their manifestation (e.g., second-and-a-half generation wireless). Finally, remote access methods should complement normal network methods should the latter be unavailable in crisis or emergencies. Both wire line and wireless access to DOJ's SBU network should be viewed as a Virtual Private Network, tunneled through the Internet, connecting a PDA or computer to the Department SBU network, and providing SBU-level encryption for traffic in the tunnel.

Strategy

Understanding and satisfying comprehensive data communications requirements for all of the DOJ's components is no small task. The input of each DOJ component is critical. This statement of telecom strategy does not pretend to be a comprehensive set of requirements for a Department network. However, the following strategy reflects requirements that would be part of any complete set of requirements for a Department network.

Appendix D
Telecommunications Strategy White Paper

Create a Department network that provides one transport fabric. A Department network should not require provisioning of either real or virtual circuits to implement sharing of applications or data by DOJ components, if their offices are already provisioned with access to the Department's national network. At present, DOJ components' networks do not meet this requirement. A Department network must be based on one, DOJ-wide, national backbone network (potentially assembled from multiple supplier's networks to assure competition and redundancy). The existing DOJ component national backbones should be combined into one national backbone. Such a national backbone should have sufficient performance and redundancy to meet both the operational and contingency plans for the DOJ, as a whole. Performance and continuity of operations should be examined and implemented at the Department level. The backbone must satisfy a consistent DOJ policy for providing performance and continuity of operations that meet the needs of *all* of the DOJ's components. Decisions about the capacity and redundancy used to connect an individual office to the backbone can be tailored to the specific needs of an office connected to the backbone.[1]

Create a Department network that provides one service fabric. A Department network should provide adequate performance for *best effort* data services.[2] It should also be able to support video services, and IP-enabled voice services with a single network, anticipating that DOJ components will develop the business cases justifying such services. Such services have more demanding performance requirements than best effort data services.

Create a Department network that provides a DOJ-wide approach to protection against external threats. As a matter of policy, all on net, DOJ data (including video and voice) traffic should be considered to be at least SBU. The transport fabric should encrypt all data carried over public facilities (i.e., a supplier's network providing the wide-area data services used to implement a Department network) using commercially available, NIST and NSA certified encryption products. There should be a Department policy governing the exchange, filtering, and monitoring of traffic with non-DOJ networks interconnected with the SBU network. This enables clear accountability at the Department-level for defense against external threats. Type I encryption should be added to support mission specific needs. Classified networks and networks used to connect to external partners (e.g., CJIS) should ultimately transition to VPNs within the overall DOJ network. The classified networks would have an additional layer of encryption and be tunneled through the SBU network. There should be a Department-level policy governing the interconnection of the Department SBU network with classified networks and the CJIS network that establishes clear, Department-level accountability for the implementation of the policy.

[1] Access and backbone redundancy should consider VSAT technology as an element of the Department network. In addition to path diversity that reduces common failure modes (e.g., damage from an earthquake), VSAT technology may be the most cost-effective way to reach some remote offices (e.g., those associated with the border patrol and immigration).

[2] *Best effort* data services are those provided by the IP protocol. The transport network makes no guarantee that a packet will be delivered. Applications must choose to use an end-to-end protocol such as TCP to guarantee delivery of a packet.

All forms of remote access to the DOJ’s SBU network raise security issues. The Department network should access the Internet from a controlled number of points (for redundancy of the service) subject to a common policy for exchanging, monitoring and filtering of traffic. VPN access (tunneled through the Internet) to DOJ’s IP networks should follow suit. A VPN (tunneled through the Internet) should extend dial-in access to include common forms of broadband access and wireless access. A wireless VPN gateway should be a DOJ-wide service. It should be centered on support for commercial off-the-shelf wireless data devices, e.g., the RIM Blackberry. DOJ should also specify a DOJ standard PDA and mobile computer configuration that implements a secured VPN.

Recommendations

The DOJ should phase out the JCN and the Metropolitan Area Network (MAN), and apply lessons learned to the implementation of a Department data network.

- PVCs are not cost effective. The JCN has demonstrated that it is not possible to rapidly deploy either (permanent) virtual or real circuits to accommodate a new configuration of an application and its clients. PVCs do not scale with new applications that are required by DOJ components. For example, a full mesh of PVCs is required to provide the performance and connectivity the EOUSA requires between its PBXs to implement an converged IP backbone for its voice and data services.
- Currently, many DOJ components staff a Network Management Center (NOC) for their national networks, and these functions are duplicated by the JCN network management center. Each of these DOJ-managed NOCs must be coordinated with the network supplier’s (Sprint) NOC. This has proved to be continual source of frustration and confusion in managing network outages and configuration changes. The DOJ does not need to operate a NOC at either the component or department level. Managed network services are widely available from multiple suppliers. The DOJ should rely on its suppliers and Service Level Agreements (SLAs) to assure a well-run network.
- Unpredictable billing makes budgeting for data communications difficult for the DOJ and its components. The present system needs to be replaced by a funding mechanism that makes budget planning predictable at all levels of the DOJ.

The DOJ should fully outsource the implementation and operation of a Department network. Transport services are a commodity. The DOJ’s costs associated with designing, operating and managing network elements duplicate costs already incurred by the supplier. The DOJ and its components should not duplicate network services (such as NOCs, managed network elements, etc.) already available from multiple suppliers. The outsourced network should include edge or premises devices that are located at DOJ facilities. In addition, the DOJ should procure, but outsource the operation of, the Type I encryption devices it uses to implement classified networks as VPNs running over the outsourced SBU network. The Local Area Networks (LANs) within a building should be the point of demarcation between DOJ component run facilities and the outsourced Department data network. (Note: the DOJ should consider outsourcing the

Appendix D
Telecommunications Strategy White Paper

operation of in-building LANs as well.) Figure 4 illustrates the minimum set of concepts that should be outsourced.

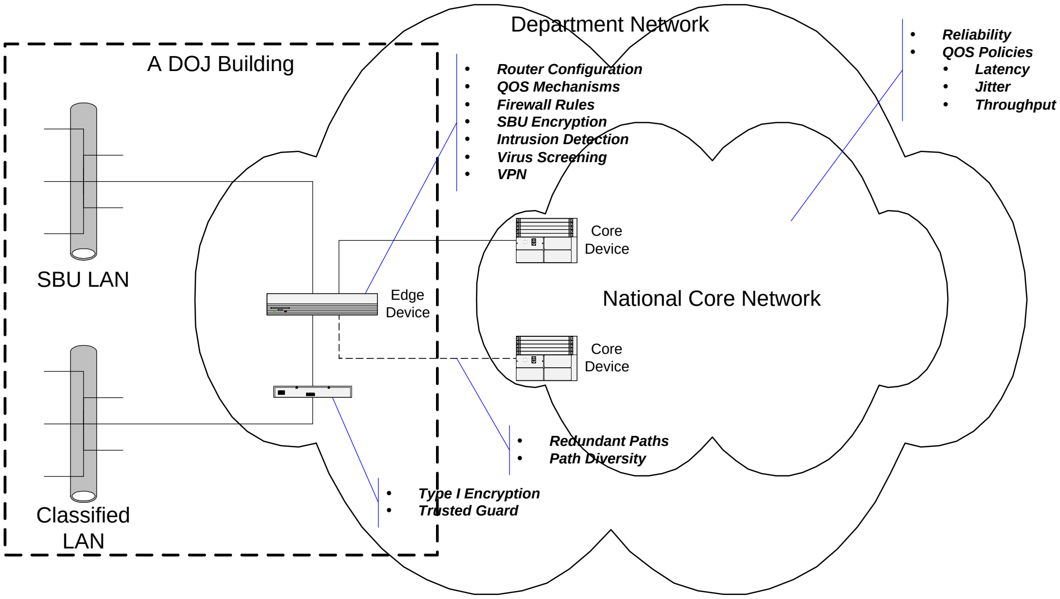

Figure 4

Concepts to Outsource

The national core network shown in Figure 4 should be designed to be highly reliable, meeting the overall needs of a Department-level continuity of operations plan. Access to this core network from individual buildings can be adapted to meet the specific needs of the DOJ components that are tenants of a building. A component with a continuity of operations plan that can tolerate or shift operations to another location in the event of a failure of an access path may chose to have a single physical connection to the national core network. A component with a continuity of operations plan that requires network access as long as a building is functioning may chose to deploy redundant, diverse paths connecting it to the core network, as suggested by the second dashed line between the edge and core devices shown in Figure 4.

DOJ component-level responsibility should be shifted to the Department-level (in consultation with DOJ-components) for several key deliverables. These deliverables include:

- Requirements for *one* Department network
- Development and execution of a transition plan for DOJ component networks to a Department network
- Development and execution of an acquisition plan for a Department data network

The Department, in consultation with its components, should assemble and hold accountable a single organization responsible for contract management related to the operation of a Department network with special emphasis on the skills needed to:

- Write and evaluate Request for Proposals (RFPs)
- Write, monitor, and enforce SLAs

- Perform configuration management
- Perform traffic monitoring, analysis and forecasting
- Perform reliability monitoring, analysis and forecasting

In order to implement the data network portion of the Information Technology Strategy, the DOJ should revisit and revise the model it uses to fund data networks. The DOJ must first develop a plan for funding the transition of multiple data networks to a Department data network.

The DOJ should also develop a plan for sustained funding of a Department network. This plan must be consistent with the goals of clear accountability for end-to-end communications, and assure that the network provides the characteristics of a Department utility that enables information sharing. This means agreeing on a Department network that meets or exceeds *every* DOJ component's requirements for security, performance, and continuity of operations, and developing a plan for satisfying those requirements.

The DOJ should create a Program Management Office (PMO) for the Department network. The PMO would be the single point of accountability for the network. The PMO should be staffed at the DOJ-level. It should be based on an "all star" team of technologists and contract administrators drawn from multiple DOJ components and contractors. The PMO should employ industry "best practices" for enterprise network development.

A Department network should be developed by first creating a national, SBU network to support the EOUSA and one other DOJ component. The EOUSA has some of the most sophisticated requirements for data networks (data, video and voice services), and has the most aggressive schedule for revising its network to meet its evolving requirements. The EOUSA's requirements cannot be met cost-effectively by the JCN.

The SBU network should support at least two DOJ components from the start. This would assure that the DOJ develops the processes, management teams, and suppliers that can meet requirements from more than one DOJ component. Candidate partners for the EOUSA include the USMS and the INS. The USMS must reach most of the same geographic locations as the EOUSA. The USMS needs to significantly improve its network infrastructure to enable changes in the Prisoner Tracking System and the deployment of the Joint Automated Booking System. Both the EOUSA and the USMS would be able to focus on the principles, processes, and requirements for building and operating a Department network because of the immediacy of their networking needs.

The INS has the most extensive and difficult to implement network of the DOJ components (because of its geographic diversity). The INS would assure that initial requirements for the SBU network dealt with a large diameter network. Redirecting the INS network to a shared SBU network may be the basis for an attractive funding plan for the transition to a Department data network. The involvement of the INS would be complicated by the need to simultaneously address many other critical information technology issues in the INS.

Appendix D
Telecommunications Strategy White Paper

The DOJ should immediately reduce spending on the JCN. It can do so by reducing the JCN NOC and DOJ components' NOCs that duplicate services already provided by Sprint. The DOJ should invest its efforts to monitor and enforce Sprint's compliance with its Service Level Agreement during the transition period to a Department network. As the EOUSA leaves the JCN, the DOJ should reduce the JCN circuits provided by Sprint to be better match to the reduced needs of the DOJ components temporarily served by JCN.

After the initial Department network is established to support the EOUSA's and one other DOJ component's operations, the DOJ should expand the implementation of the SBU network to include all other, non-classified DOJ networks. This will require developing and funding a transition plan that moves each remaining DOJ components' operations to the new network, and completely phases out the JCN and the MAN.

Once a DOJ-wide SBU network is constructed and operational, DOJ should then expand it to carry mission-specific, classified network traffic. The approach should use the SBU network as a national backbone for classified VPNs implemented by Type I encryption as traffic leaves and enters classified DOJ office spaces. Since the entirety of the FBI's network (Trilogy) is classified, the FBI would be the last DOJ component to move its primary network to a Department network. This has the advantage of assuring that the major upgrade undertaken by Trilogy has been completed and stabilized before a transition takes place.

As a last step, the Department network should be expanded to provide the underlying transport for the CJIS network. As with classified network traffic, an implementation of the CJIS network should be a VPN. CJIS delivers connectivity for non-DOJ law enforcement agencies and should be logically separated from the SBU network that serves the DOJ's internal needs. Unlike the SBU or classified networks, the CJIS network has a governing board that comprises representatives of state, local and tribal law enforcement organizations. This board would need to have its requirements met as CJIS is transitioned to a Department network.

DOJ should anticipate and quickly respond to the need for wireless and remote access to the DOJ's network. DOJ should invest in short-term security mechanisms, and adequate network and encryption capacity to assure that wireless and other forms of remote access to DOJ's IP networks can be encrypted at a level suitable for SBU traffic, and without performance impact.