



JUTNet Managed Network Service

Transforming Disparate Telecommunication / Network Infrastructures at DOJ to an Enterprise-wide
Managed Network and Security Service

February 15, 2011

Shirley Nasser
Department of Justice
JUTNet Program Director
Office of the Chief Information Officer
Shirley.Nasser@usdoj.gov
202.353.7688

Executive Summary

Federal IT leaders should consider use of a managed service model when evaluating alternatives for consolidating technical infrastructures (e.g., telecommunications, datacenters, e-mail) as significant cost benefits and efficiencies can result. Off-loading complex technical details to an experienced and skilled enterprise-class managed service provider translates to financial and technical benefits and redeployment of assets to better serve the agency's mission.

The Department of Justice, via an acquisition procurement, engaged a single managed service provider with end-to-end responsibility for security and networking to consolidate numerous DOJ component WANs. By aggregating multiple DOJ component WAN requirements into a unified enterprise infrastructure, compliance with Federal IT policies, standards, and directives such as TIC, IPv6 and FISMA became efficient and less costly than performing the work independently for multiple component networks. Government purchasing power improved by aggregating the separate expenditures and provided leverage to negotiate aggressive service level agreements with strong financial penalties for non-performance.

Challenge

The United States Department of Justice (DOJ) is comprised of approximately 40 diverse components, bureaus, and offices that have been historically united by a common law enforcement mission. DOJ components include the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Federal Bureau of Prisons (BOP), Drug Enforcement Administration (DEA), the U.S. Attorneys, and the U.S. Marshals Service (USMS).

Prior to implementation of the Justice Unified Telecommunications Network (JUTNet), many DOJ components had separate IT organizations and resources in place to manage their own Wide Area Network (WAN), with each team employing distinct approaches to the architecture, management, and security of their network. Furthermore, DOJ components were individually responsible for Certification and Accreditation (C&A) activities and complying with increasingly complex federal policies and standards. To perform the necessary telecommunications, networking, and security work, each DOJ component relied on a range of technical subject matter experts and business resources.

In the post 9/11 environment where timely establishment of temporary communication channels between DOJ components became a mission imperative, especially in support of counter-terrorism activities, the continued operation of multiple fragmented heterogeneous networks was no longer acceptable. A far more efficient approach was needed to meet DOJ's information sharing and security requirements and comply with Federal IT directives programmatically.

Solution

The Department embarked on an extensive effort to survey the DOJ components, other Federal agencies, service providers, system integrators and leading technology adopters to identify best practices, proven solutions and lessons learned. The resultant JUTNet solution is an enterprise-wide shared service that integrates managed network services, managed security services, and alternate carrier services under a single provider umbrella that satisfies DOJ component, Department, and Federal IT requirements.

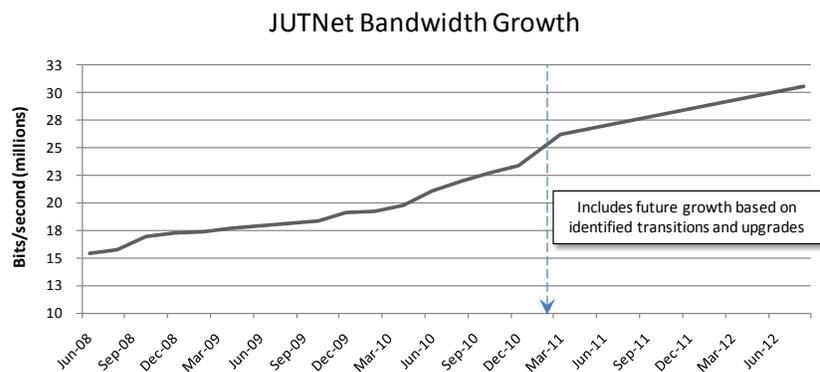
JUTNet provides end-to-end connectivity via a standards-based IP network, an equipment set at each DOJ location, and a suite of modular pre-defined service configurations to simplify configuration management and streamline service delivery. Numerous security features are integrated into the network architecture and management including managed firewalls at each location, dynamic multipoint VPN technology to provide secure connectivity between any two network end-points, and intrusion detection and protection services. All C&A activities and compliance with Federal IT standards and policies are addressed by the managed service provider. DOJ components have access to the provider's 24x7x365 Network Operation Center (NOC) and a comprehensive set of web-based business and operational support systems that provide customized views of their virtual network.

To eliminate confusion that could result from distributed or shared responsibilities, the service provider is solely tasked with end-to-end management of the network service and the security service. The provider owns and operates all elements in the network infrastructure including local access and end-point equipment at DOJ locations, NOCs, and business / operational support systems.

Results

JUTNet is one of the largest successful IT infrastructure transformation programs at the Department of Justice. Today, the managed enterprise service provides data connectivity to over 2,100 DOJ datacenter, headquarters, and field offices throughout the continental United States and its territories. The network also provides connectivity to over 500 Federal, State, and local law enforcement organizations.

The JUTNet architecture provides data, voice, and video services, is fully compliant with Federal IT standards and policies, and provides DOJ with the ability to respond to new requirements and mandates in a cost-effective and efficient manner by dealing with one common infrastructure. By relying on the managed



service provider to handle technical details, more resources are available to fulfill mission requirements.

By aggregating DOJ component telecommunication and network expenditures, the Department was able to negotiate favorable contract terms and conditions with the provider and establish strict performance based service level agreements with financial penalties that cover all aspects of service assurance and service delivery. Components have leveraged the network to take advantage of features and functionality that in many cases would have been cost-prohibitive, too time consuming, and /or require additional technical expertise for each component to acquire and implement on their own.

Lessons Learned

- A managed service model should be considered for enterprise-wide IT projects (e.g., WAN, E-mail, datacenter consolidation) where economies of scale and efficiency can result from having a homogeneous baseline infrastructure.
- Aggregation of multiple DOJ component WANs into a unified enterprise infrastructure made timely compliance with Federal IT directives (e.g., TIC, IPv6, FISMA) feasible, efficient and cost-effective.

- Establishment of aggressive provider SLAs with substantive financial penalties for non-compliance is vital to driving desired network performance levels and behavior.
- Unwavering OCIO and senior management leadership and support is a critical factor for success in the acquisition of large transformational IT infrastructure initiatives as the need exists to routinely navigate through substantive internal and political obstacles.
- Engage key stakeholders from the onset and ensure they have representation throughout the project – from requirements definition to vendor evaluation – as this will improve the final solution and temper challenges including resistance to change.
- Invest time early in the planning stage to develop solid business and technical requirements that incorporate best practices from a variety of sources.
- Establish an architectural and governance framework that will support growth and change since requirements will evolve no matter how exhaustive the preparation efforts.
- Understand the financial impact on each community that moves to the shared model and be cognizant of equitability since not everyone will benefit identically.

Related Information

The JUTNet Program Management office can address questions and share Best Practices with Federal agencies that are contemplating transition to an enterprise-wide managed service model. For additional information, contact Shirley Nasser (Shirley.Nasser@usdoj.gov; 202.353.7688).

Disclaimer

References to any product and/or service names of the hardware and/or software products used in this case study do not constitute an endorsement of such hardware and/or software products.