

**PART III – LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS**  
**SECTION J – LIST OF ATTACHMENTS**  
**J.9 – NAIS I-2 COMPONENT DESIGN CONSTRAINTS**  
**ENCL.4 – DHS ONENET**

---

**DHS OneNet Overview**

Background

In its effort to transform the IT Infrastructure to meet the requirements of department wide information sharing, the Department of Homeland Security (DHS) has implemented the Infrastructure Transformation Program (ITP). The ITP calls for the department to consolidate its Sensitive but Unclassified (SBU) networks into one department-wide network backbone. The ITP's goal is to consolidate the department's 16 component-level data centers into two department-wide data centers to provide the required availability and survivability, and to consolidate component SBU networks into a single network, called "OneNet." The Customs and Border Protection (CBP) agency has the responsibility for DHS' OneNet network infrastructure under the ITP plan.

Network Architecture

DHS is developing an Enterprise Architecture (EA) that will help guide the creation of a unified core of human, business, and technical resources to perform its mission to "Secure the Homeland, its people, assets, and interests." The emerging DHS OneNet will support communication and interaction among many organizational entities within and outside of DHS. The network will be designed to support all communication types including, but not limited to, voice, data, video, tactical radio, and satellite. The network will support the Internet Protocol (IP) Version 6 suite of protocols and operate over two service provider networks, through the use of Multi-Protocol Label Switching (MPLS) technology.

Network Monitoring and Security

DHS is adopting a defense-in-depth with a multiple layers of security approach to securing OneNet and its enterprise. The DHS network infrastructure protection will be the responsibility of the DHS Network Operations Center (NOC) and the DHS Security Operations Center (SOC). The NOC will be responsible for ensuring the reliable operation of the enterprise network. In this role, the DHS NOC will manage the configuration, operation, monitoring, and maintenance of the entire network infrastructure and will be supported by a network management system and a suite of network devices. The DHS SOC will be responsible for monitoring the security of the enterprise network, corporate servers, and desktop systems. In this role, supported by a Security Information Management system, the DHS SOC will manage the configuration, operation, monitoring, and maintenance of security devices deployed around the enterprise. The DHS NOC and DHS SOC will manage the resolution of incidents in their corresponding domains of responsibility, network functionality and security, respectively, on a 24x7x365 basis. The tools employed by these groups range from vulnerability scanners to enterprise-level management systems, which collect and aggregate data feeds and act as a central focus for their efforts. The exact nature of the security architecture is beyond the scope of this document.



**PART III – LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS**  
**SECTION J – LIST OF ATTACHMENTS**  
**J.9 – NAIS I-2 COMPONENT DESIGN CONSTRAINTS**  
**ENCL.4 – DHS ONENET**

---

Enterprise Application Support

DHS has purchased Microsoft enterprise licenses, and DHS organizations are expected to use Microsoft technology wherever possible. Microsoft products selected as standards, or being considered, include: Microsoft Exchange for e-mail server software; Microsoft Outlook for e-mail client software; Microsoft Office for desktop productivity standard; Microsoft and Entrust Certificate Authorities; and Microsoft Active Directory (AD) to configure and manage network resources. Note that while AD will be used as required to support Microsoft and other products that use Active Directory's service, no product has yet been chosen to serve as the DHS enterprise directory service, and some DHS organizations use other directory products.

Network Availability and Performance

The DHS OneNet is operational 24 hours a day, 7 days a week. Expected availability across all routers on the network is at least 99.9%. Expected latency between routers on the network is less than 100ms.

