TERMINOLOGY NOTE: The DoD High Performance Computing Modernization Program (HPCMP) operates 2 networks, called DREN and DRENv6. DREN is a nation-wide network, DRENv6 is a small test bed. DREN has run dual-stack for about 2 ½ years, DRENv6 is a native IPv6-only network established about 5 years ago. It is assumed in answering the questions below that they were about the DoD IPv6 pilot network, which is synonymous with the DREN. DRENv6 has been replaced by "DREN IPv6 pilot."

Questions for Decision Makers

1. What were the motivations for building and maintaining DREN IPv6 pilot?

In the DoD, the motivation was the requirement to support future warfighter capabilities in an affordable manner, while providing new functional capabilities. The DREN IPv6 pilot supports the DoD research and engineering community. This is a leading edge community that continuously looks at technologies that may eventually become important to the Department of Defense; IPv6 is one of those technologies. Complex battlefield communication environments, more secure communications protocols, mobile telephony, class of service requirements will all be enabled by this technology in some significant way in the future. And this technology will be used by potential adversaries. We wanted to flush out methodologies for ensuring that IPv6 doesn't circumvent current security perimeters before there's a need, not after.

2. Was there a business case for building DREN IPv6 pilot?

It's very difficult to build a real business case since, in effect, there are no additional capabilities in IPv6 that are available today, that can't be done some other way using IPv4. Then, adding the burden of flushing out weaknesses and incompatibilities in vendor implementations makes it difficult to find a positive return in a reasonable timeframe. The mitigating counter argument is, that it's not that expensive to do what we've done. A few smart people, relatively homogenous platforms at our shared resource centers, a centrally controlled wide area network, and congruent objectives across the Services all contributed to allowing us to implement both a national scale test bed and production network at an affordable cost.

3. How does DREN measure the value of DREN IPv6 pilot?

This is a question that might be better asked to others in DoD or Federal Agencies since we've been the enabler for others to start moving towards solutions i.e. rapid deployment of the DoD MoonV6 testing (www.moonv6.org), a real example of how to do a nationwide addressing plan, and other lessons learned given to both DoD and other Federal Agencies.

4. DREN is currently operating DREN IPv6 pilot and an IPv4-based network. Has DREN observed any differences in resource allocation or management?

Impacts have been minimal. As a DoD network, we had to ensure that whatever was being done for security in IPv4 environments was also done for IPv6 as part of the DREN IPv6 pilot. The DREN IPv6 pilot is an in-place upgrade of the previously existing IPv4-based network. There have been no observed differences in resource allocation, and minor increases in management effort since upgrading the DREN to the DREN IPv6 pilot. Existing IPv4-based network management tools, at least in the United States, often lack equivalent IPv6 capabilities. We continue to add/expand our suite of network management tools as IPv6 products/features become available.

Please refer to section 13 of the attached **IPv6 Transition Survey Questions.pdf** document for information about router upgrades that occurred as part of the DREN IPv6 pilot.

5. It is DoD policy to transition to an IPv4/IPv6 environment by 2008, what are some lessons from the experience of DREN that will be applied to the dual-stack environment of the DoD?

Please see the attached document. It provides information about lessons learned described in an earlier questionnaire from v6 Transition.

6. Through what metrics does DREN measure the progress of DREN IPv6 pilot and have the goals of DREN IPv6 pilot been achieved?

The DREN IPv6 pilot had 5 main goals when it was established in 2003, and has completed or substantially completed them. As for metrics, see section 8 of the attached document.

Questions for System Administrators

1. How many nodes and users of DREN IPv6 pilot are there today? How large does DREN expect to grow DREN IPv6 pilot?

See section 1 of the attached document for nodes and users for the entire DREN IPv6 pilot. The DREN IPv6 pilot can grow with the DoD research and engineering communities' needs for IPv6 access. At an individual site, the Naval Research Laboratory – District of Columbia (NRL-DC), there are presently over 150 nodes available across the laboratory, for example.

2. What additional training in administration and security was given to users of DREN IPv6 pilot? Has this changed since the system was first built?

Users received no additional administration and security training. System administrators and network managers did receive additional training, as described in section 4 of the attached document. In addition, the DREN IPv6 pilot established a knowledge base web

site for use by DREN IPv6 site personnel. There have also been tutorials provided at annual DREN Networkers Conferences on IPv6 technology and security. At individual site, the NRL-DC for example, local network managers and system administrators were further briefed on IPv6 as laboratory wide implementation occurred, and site specific documentation was provided online.

3. DREN continues performance testing of IPv6 over DREN IPv6 pilot. What are the results of tests of IPv6 performance of typical network tasks – e.g. ping, traceroute? What are the results of tests of IPv6-specific tasks – autoconfiguration, flow labeling, use of extension headers, etc.? Have any of the results been surprising?

Performance of IPv6 and IPv4 are essentially equivalent, in both throughput and latency, for typical network tasks. The purpose of the DREN IPv6 pilot was to provide functional equivalency with the previous IPv4-only network. As such, IPv6-specific capabilities such as those mentioned were not implemented or tested. No.

4. IPv6 offers a vast address space, has DREN IPv6 pilot experimented with alternate methods for allocating addresses?

No, it has not.

5. Since the construction of DREN IPv6 pilot, there have been several viruses targeted at networks using IPv4 for routing. Has DREN IPv6 pilot suffered at all from these attacks, especially in its connections to external networks that use IPv4 tunnels?

The previously existing IPv4-only network had good protections in place against such attacks, and the DREN IPv6 pilot has equivalent protections. We have observed no differences in the consequences of attacks between the two.

6. What lessons does DREN IPv6 pilot offer in the use of IPSec over IPv6, including establishing security associations and issues with respect to key management?

The DREN IPv6 pilot has not attempted to use the IPSec features of IPv6 for end-to-end communications on a regular basis. We have performed limited scale technology evaluations and participated in tests such as the previously mentioned MoonV6. It is important to realize that IPsec is not something that is new to IPv6. IPsec is currently available, in fact, is more widely available, for IPv4. IPv6 just mandates that IPsec be implemented as part of the IPv6 stack.

With that noted, there are not too many IPv6-specific issues regarding IPsec. We have found that IPsec implementations for IPv6 have been slow coming to market. Most major OSes have had an established IPsec implementation for IPv4 before an IPv6 implementation was available. IPv6 implementations are still maturing and will take some time (due to limited use) to become stable. Please realize exactly what IPsec can do and don’t attempt to use it to solve other problems. IPsec is a host-based security mechanism and does not authenticate the user (although some implementation-specific

extensions may allow the network to authenticate a specific user). Application security is still a critical concern as are other traditional threats (social engineering, physical security, etc). Remember that a virus or worm can be spread via an encrypted IPsec tunnel just as readily as by an unencrypted connection. The only difference is that your IDS/firewall will not see it propagating.

IPsec issues that are common to IPv4 and IPv6:

Key management: This is requirement is often underestimated and critical to the success of any IPsec deployment. The DoD PKI provides a solid foundation for key management and makes IPsec deployment much less daunting. Non-DoD agencies that do not have such an infrastructure may face significant challenges in effective key management.

Mis-use of IPsec: Many organizations have a bulk of their security policy built into a perimeter defense implementation (firewalls, IDS, etc). IPsec can effectively bypass the traditional perimeter, requiring multiple implementations of the perimeter defense mechanisms or a change in the approach to implementing security. The use of IPsec should be managed appropriately in this respect such that perimeter defense security measures can be equally applied to tunneled traffic. IPsec tunnels that are not subject to analogous perimeter defense measures may need to be disallowed by policy.

Administrator Interface: IPsec is a complex protocol and needs to have a user-friendly interface in order to be effectively used. The lack of common interfaces and common features among different OS implementations will induce error-prone and ineffective deployments. The new IPsec protocol specifications (IKEv2) hold promise for simplifying the administration interface.

How we will use IPsec: Most of today's IPsec deployments are in VPN products and rarely based on the OS IPsec capability. It is not clear that we will want to continue to use IPsec in the form of appliances and specialized hardware. Experience from IPsec-based VPN products show that vendor-specific extensions and limited common feature support are not delivering the ubiquitous security infrastructure that is a desired goal for IPsec and IPv6 across DoD networks.

7. According to a recent NIST study, the transition to IPv6 will take over 20 years, which means that many companies will be operating a *de facto* dual stack environment for a long time. How is DREN's test program preparing it and the DoD for such a state of affairs?

The DREN IPv6 pilot was implemented from the beginning as a permanent change in the architecture and operation of DREN, not as a test program. The HPCMP has consistently and persistently documented and disseminated lessons learned from the implementation of the DREN IPv6 pilot to the DoD community.

8. How does DREN use its relationship with partner networks – e.g. Moonv6, 6bone – to improve its operation of DREN IPv6 pilot?

As part of its security architecture, DREN has isolated all peering with external IPv6 networks, including MoonV6, 6bone, Internet2, *et cetera*, onto the DRENv6 test bed. It has maintained and expanded the number of external peering relationships with other IPv6 networks in order to provide the best possible connectivity to the wider IPv6 world for the DoD research and engineering community. At individual sites, such as the NRL-DC, local researchers collaborated on early 6bone efforts and Moonv6 projects in the past, and such early research efforts helped to drive initial requirements for IPv6.

Questions for System Users

1. Do you feel that the training you received in IPv6 was sufficient to use fully the features of IPv6? How is the nature and purpose of the training different than that for IPv4?

[an answer from a network providers perspective] Users should not require any training in IPv6. Software developers do require training, but the DREN IPv6 pilot did not address this audience. It is not expected that there would be any difference in the nature and purpose of such training.

2. What additional training in security did you receive and do you feel that it is sufficient? When DoD transitions to a dual-stack environment, do you feel that the security of DoD networks will become easier or harder to manage?

[an answer from a network providers perspective] Users should not require any security training specific to IPv6. In a dual-stack environment, the security of DoD networks will tend to become harder to manage. This increase will be comparable to occasions in the past when multiple protocol suites were supported by a single network, such at Novell or AppleTalk with IPv4.

3. Are there and special features of IPv6 that you use often: autoconfiguration; multicast, unicast, and anycast traffic; flow labeling; etc.?

[an answer from a network providers perspective] Users should not be particularly aware of how their applications gain increased functionality. Whether a system is using IPv4 or IPv6 should be transparent for users. Software developers will be keenly aware of such special features, but the DREN IPv6 pilot did not address this audience.

[At an individual site, NRL-DC] They are using stateless autoconfiguration. Users/ system administrators have been provided with instructions on how to configure their systems in the NRL-DC environment.

4. IPv6 boasts a simplified header structure and implementation. Have you measured performance differences between IPv4 and IPv6?

[an answer from a network providers perspective] Beyond the performance measurement described under number 3 in **Questions for System Administrators**, no.

5. Given your experience with DREN IPv6 pilot, how well do you think IPv6 will address the future needs of the DoD, especially in areas of mobile telecommunications?

[an answer from a network providers perspective] How IPv6 will ultimately address the future needs of the DoD after IPv4 has been phased out is difficult to predict, because that is several years in the future. In the near term, while all DoD networks will be operating as dual-stack implementations, it should at least be able to provide equivalent functionality. Large-scale implementation of IPv6-specific features such as mobility may be difficult to accomplish on such dual-stacked networks.

6. Given your experience with DREN IPv6 pilot, do you feel that IPv6 will usher in a new era of Internet communications, or is IPv6 a needed replacement for IPv4?

[an answer from a network providers perspective] IPv6 is a needed replacement for IPv4.