Draft TIC Teleconference Minutes
December 18, 2007

I. Participants

Scott Behula		
Don Bonack	DHS	
Joe Burrescia	ESnet	joeb@es.net
Rich Carlson	Internet2	rcarlson@internet2.edu
Bobby Cates	NISN	
James Cook	DREN	jrcook@hpcmo.hpc.mil
Vince Dattoria	DOE/SC	Vince.Dattoria@science.doe.gov
Phil Dykstra	DREN	
Jim Gagliardi	DOE	
Andy Germain	NASA	
Mike Gill	NIH/NLM	
Ken Goodwin		
Chris Greer	NCO	greer@nitrd.gov
Dave Hartzel	NREN	david.hartzell@nasa.gov
Hugh LaMaster	NASA	
Annabelle Lee	DHS	
Paul Love	NCO	epl@sover.net
Dan Magorian	MAX	
Joe Mambretti	StarLight	j-mambretti@northwestern.edu
Allison Mankin	NSF	
Bill Marsh	NSF	
Ernest McDuffie	NCO	
Grant Miller	NCO	miller@nitrd.gov
Bill NicklessPeter O'Neill		
Mike Rechtenbaugh	USGS	
Bill Semancik	NSA	
Bill Turnbull	NOAA	Bill.Turnbull@noaa.gov
Randy Vickers	DHS	Randal.Vickers@dhs.gov
Alan Verlo	UIC	darkman@evl.uic.edu
Linda Winkler	StarLight	

Action Items

1. JET will continue to discuss the TIC requirements, cooperation with DHS/OMB, and implementation issues.
2. NGIXs offer to serve as development and test sites for TICs
3. DHS will consider additional representatives from the Federal research agencies on its architecture committee
4. Bobby Cates (NASA) and Randy Vickers (DHS) will serve as POCs for continuing questions on research network compliance with TIC requirements.

Proceedings

This teleconference provided discussion of the Trusted Internet Connections (TIC) memorandum issued by OMB and DHS. The OMB memo 08-05 covers all Federal agency external communications, not just Internet connections.

Randy Vickers of DHS with technical support from Don Bonack discussed the intent and requirements outlined in the memorandum. The memorandum sets a goal of 50 peering sites among the Federal agencies for connectivity to the general Internet. The goal is 50 points but agencies should architect themselves to the number of sites that makes sense for them. Agencies are expected to develop a plan for reducing their number of peering points with the general network and to show due progress toward this reduction. The peering sites will be architected and protected to provide trusted points for access to and from Federal agency resources. DHS will be developing conceptual architectures for these points and will be considering technologies to implement port protocols, security architectures, IDS, stack protocols, and other capabilities. Einstein security will be one of the requirements.

Each of the Federal agencies is expected to develop an architecture including connection points with the required security. That agency assumes responsibility for managing those points. If an agency can not afford to establish and maintain its own connectivity point, it can cooperate with another agency to implement rusted Internet Connections.

Contractors with Federal agencies have security requirements as part of their contracts with the government and implementing those contractual obligations may be sufficient so that they do no9t need a TIC. Lockheed Martin coordinating with the University of Chicago over the Internet, and not going through the Federal agencies will not require a TIC. The contractor, contacting the Federal agency through the Internet does provide entry into Federal resources and would need to go through a TIC.

Inter-Federal agency Internet communications have to go through a TIC. NASA contacting DOE would go from the NASA source through the NASA TIC to the DOE TIC to the DOE destination. Intra-Federal agency communications, e.g., DOE Lab 1 to DOE Lab 2, do not have to go through a TIC.

A DOE university site going to a HEP center (e.g., Fermilab) would use a point to point link and would be isolated from IP traffic. However, if the site (Fermilab) has other IP connectors where the Layer 2 link lands, there would need to be security to isolate the traffic.

TIC architectures are currently under development. An architecture committee is being established (Bobby Cates is a membe). A TIC could be located at a Telco hotel and could support multiple connections to ISPs. If an agency has tail sites, they need to terminate in a TIC. NASA has a large number of tail circuits that would be affected.

Aspects of the architecture will include:

- Einstein monitoring
- Layered in tiers to provide a DMZ and Layer 1-7 access control and monitoring
- Architectural isolation of internal and external traffic

The architectural committee is currently considering what are current best practices at the perimeter: IDS, firewalls.

Requirements for the agencies include:

- Implement Einstein monitoring
- Reduction of the number of direct Internet connection points and show progress each year.
- Start implementing the TICs
- Mid January, 08 an initial architecture for each agency is needed to start identifying potential for consolidating TICs.

The TIC certification process is to be determined.
There is no funding for implementing the requirements of this memorandum; it is a non-funded mandate.

Next Generation Internet Exchange points (NGIXs)

Federal research networks maintain three NGIX interconnect points; one is Federal and two are located at universities. In addition MANLAN and the Seattle GigaPoP provide two additional research network points of connectivity. DHS will consider whether the non-Federal sites could become certified and become TICs. Discussion identified that the NGIXs represent unique and challenging sites with a wide range of demands and capabilities (Layer 1, 2, and 3; heterogeneous networking; 10 G and lambda links). The NGIXs offer to serve a test and development sites for the TIC capabilities.