Defense Security Service

Interconnected Systems

(Tito Cordero)
(DSS Irving Field Office)
(16 April 2008)

- **Purpose**
  - To provide descriptions on how to Identify different types of Network configuration or types.
  - Implement systems certification of the National Security Information at Protection Level 1 or Protection Level 2
  - Present information for Industrial Security Representative of Network documentation for LAN WAN configuration

- **Network Types**
  - Peer-to-peer - Computers can provide resources (act as server) or access resources from other computers (act as client). Used for 2 to 10 computers
  - Server based - Allow for a central control over network resources.
  - Single Server - Used for 10 to 50 users where it is wise to add a server around 25 or 30 users.
  - Multi-server - Used for 50 to 250 users.
  - Multi-server high speed backbone used for 250 to 1000 users.
  - Enterprise network has over 1000 users.

- **Network Configurations:**
  - **WAN's: The size of a network is limited due to size and distance constraints. However networks may be connected over a high speed communications link (called a WAN link) to link them together and thus become a WAN. WAN links are usually:**
  - **Dial up connection**
  - **Dedicated connection - It is a permanent full time connection. When a dedicated connection is used, the cable is leased rather than a part of the cable bandwidth and the user has exclusive use.**
  - **Switched network - Several users share the same line or the bandwidth of the line. There are two types of switched networks:**
    - **Circuit switching - This is a temporary connection between two points such as dial-up or ISDN.**
    - **Packet switching - This is a connection between multiple points. It breaks data down into small packets to be sent across the network. A virtual circuit can improve performance by establishing a set path for data transmission. This will shave some overhead off a packet switching network. A variant of packet switching is called cell-switching where the data is broken into small cells with a fixed length.**

(Protocols)

- Categories of protocols :
- Connection type
  - Connection-oriented - A protocol that relies on connection establishment between two computers. Connection oriented protocols are considered to be reliable protocols since there is a check to be sure the data was received.
  - Connectionless - Not relying on a connection. It is considered to be an unreliable means of communication.
- Routing
  - Routable - The protocol can be sent through a network router.
  - Non-routable - Cannot be sent through a network router.
- Three main commonly used protocol stacks
- TCP/IP - Routable protocol with more overhead that is used on the internet.
- IPX/SPX - Routable medium speed protocol from Novell.
- NetBEUI - Non routable fast protocol.

(Address)

- Network Type Address Range

– A001.x.x.x to 126.x.x.x	255.0.0.0	For very large networks Class
– B128.1.x.x to 191.254.x.x Class	255.255.0.0	For medium size networks
– C192.0.1.x to 223.255.254.x	255.255.255.0	For small networks Class

- D224.x.x.x to 239.255.255.255
- E240.x.x.x to 247.255.255.255

Interconnected Systems:

- There are two types of networks that DSS accredits, they are LAN and WAN. The LAN is less complex, and some IS Reps are authorized to evaluate LANs operating at PL1.

- The WAN is considerably more complex. This will require an ISSP to accredit. The ISSP can inspect PL1 (and higher) WANs for accreditation purposes.

WAN's are either Unified or Interconnected networks.

- **A Unified Network applies when all contractors and ISSPs concur that there will be a single security policy for the entire WAN. The network will have an SSP for a Unified Network that outlines all the requirements contained in NISPOM Paragraph 8-610.**

- **The host contractor will prepare an SSP for a Unified Network and include specific information for each node on the network. This may mean the nodes are identical systems where one hardware list is appropriate. The nodes may have different equipment; thus a system profile for each node may be appropriate. Because there is one security plan, and each node is described in it, a Network Security Plan or Network Security Profile is not required. Additionally, the SSP for a Unified Network must include a provision that the host must be notified before any changes are made to the system.**

WAN's are either Unified or Interconnected networks.

- The host contractor will provide the SSP for a Unified Network to the facility IS Rep, who will provide it to the responsible ISSP. The host contractor will also notify connecting nodes of the impending certification and provide them with a copy of the SSP.

- The host IS Rep and ISSP will review the SSP and notify the connecting node IS Reps and ISSPs that a Certification Process has begun.

- The host IS Rep and ISSP will complete enclosures and perform an onsite verification of the host system.

WAN's are either Unified or Interconnected networks.

The IS Reps and ISSPs for the connecting nodes are not required to complete any forms, but will take the provided documentation and perform an onsite verification that the system is as described in the documentation and that all features as outlined in the plan are compliant and fully functional. This must be accomplished within 60 days. ISSP will complete Enclosure 28, then send it via email to the host IS Rep and ISSP.

WAN's are either Unified or Interconnected networks.

- Following onsite verifications and completions of Enclosures 27s & 28s for the host and all connecting nodes, the IS Rep for the host will forward all documentation to the DAA for the host. The DAA for the host will issue a final Accreditation Letter. An Interim Approval to Operate will not be granted for Unified Networks

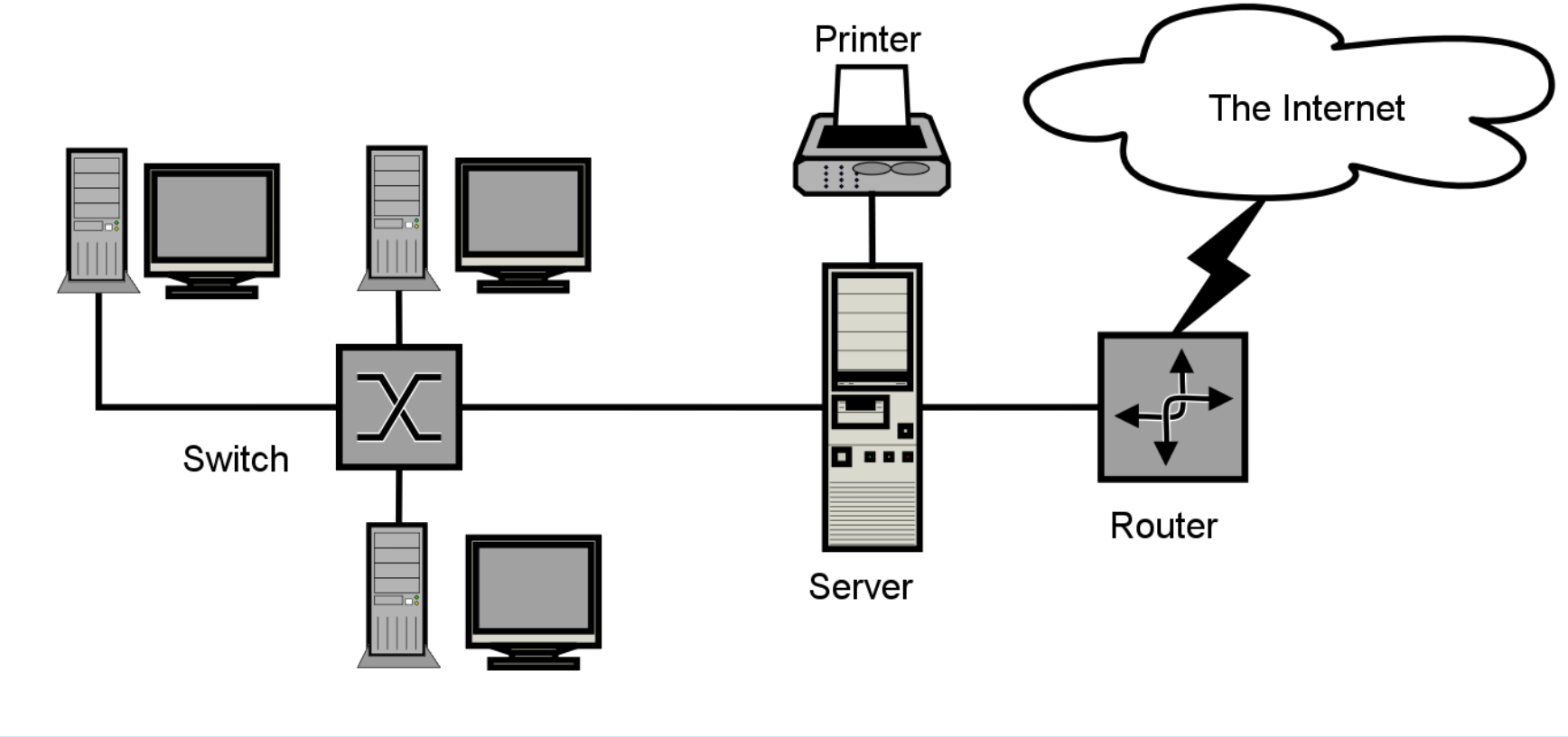
Interconnected Networks:

- An interconnected network applies when there are a number of separately accredited nodes on a network. These can be contractor-to-contractor or government-to-contractor connections or a combination of both. It is very important for IS Reps to review the clearance levels, categories and classification of the information, formal access approvals and NTK for all connecting sites. A PL1 system at one site connecting to a PL1 system at another site could create a PL2, PL3 or PL4 network. For uniformity purposes, the PL of the network will equal the PL of the highest node on the network. For example, if one of the nodes requires PL2, the network will then be accredited at PL2. However, only the node that requires PL2 will be required to meet all the PL2 requirements. Other nodes on the network that are PL1 will be required to meet PL1 requirements.

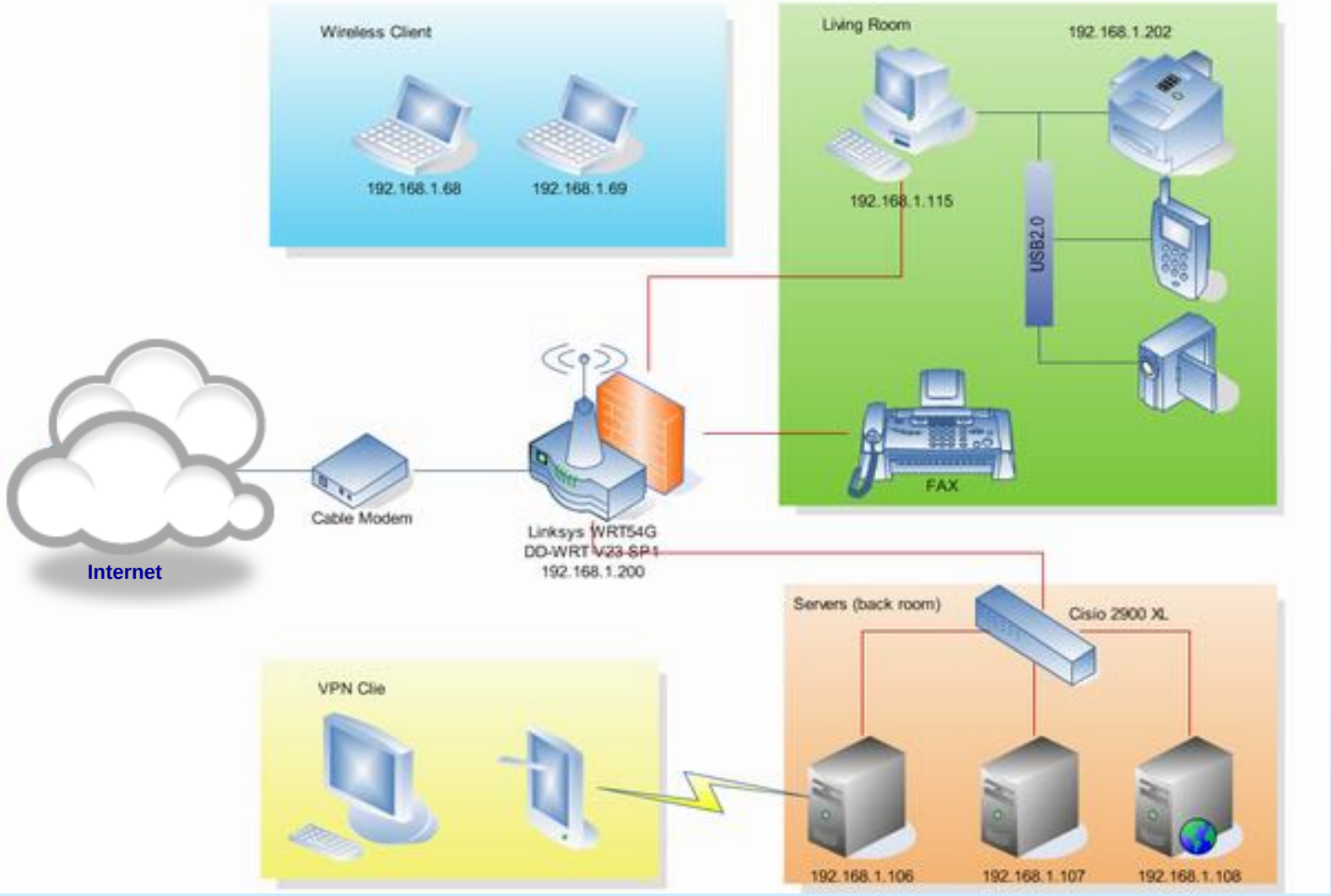
Network Security Plan (NSP)

- The network itself will have a Network Information System Security Officer (Network ISSO) (formerly called a Network Security Manager)
- Each connecting node will have an ISSM, who shall be named in the Network Security Profile.
- Include details of connections, to include remote workstations, and how privileged and general user accesses will be controlled.
- If the network will be higher than PL1, the ISSM must have the appropriate additional NISPOM requirements for the PLs included in the NSP.

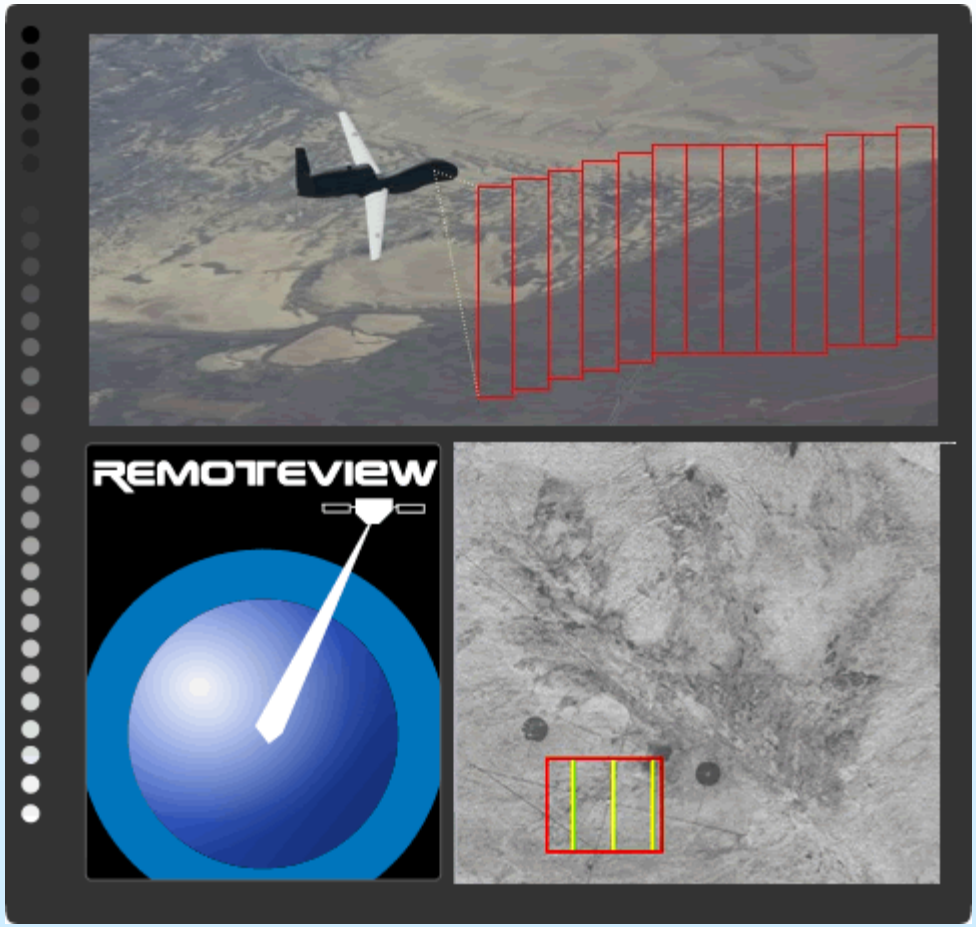
Network



(Interconnected)



(Tactical Systems)



(MOU)

MEMORANDUM OF UNDERSTANDING
Between

National Geospatial-Intelligence Agency (NGA)

and

Defense Security Service (DSS)

References: (a) NISPOM, Chapter 8
(b) DCID 6/3

This Memorandum of Understanding (MOU) between the National Geospatial-Intelligence Agency (NGA) and the Defense Security Service (DSS), Designated Approval Authority for Applied Research Laboratories: University of Texas (ARL:UT), is for the purpose of establishing a secure communications link between NGA and ARL:UT for the electronic transfer of classified information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this MOU and Interconnection Service Agreement for the Interconnection of the NGA MSN and ARL:UT MSN IS, dated 29 AUG 06, summarize the information system (IS) security requirements for approval purposes and supplements ARL:UT approved system security plan (SSP).

1. Contract Information

This MOU describes the classified network arrangement between ARL:UT and NGA in support of the Monitor Station Network (MSN). The ARL MSN IS are government furnished equipment, sponsored by NGA, used to support the Global Positioning System mission of NGA. The contract number is N00024-01-D-6660. The prime contractor is ARL:UT, whose Cage Code is 55254.

The following ARL:UT key points of contact are identified:

NAME	TITLE	PHONE
Neil Fox	Field Security Officer (FSO)	512-835-3365
Richard Mach	Project Manager/Information System Security Officer (ISSO)	512-835-3614
Lorenzo Lopez	Information Systems Security Manager (ISSM)	512-835-3755

At NGA direction, ARL:UT is establishing a remote access capability to the NGA MSN and the ARL MSN IS. The remote access to the NGA MSN is from ARL:UT-Austin. This capability will allow ARL:UT and NGA user personnel to access the NGA MSN and the ARL MSN IS as remote users.

The following NGA MSN key points of contact are identified:

NAME	TITLE	PHONE
Richard Cloninger	Information System Security Representative (ISSR)	(314) 263-4726
Lois Debrobander	Information Systems Security Manager	(314) 263-4182
Keith Ellis	MSN Program Manager	(314) 263-4149

MEMORANDUM OF UNDERSTANDING
Between
National Geospatial-Intelligence Agency (NGA)
and
Defense Security Service (DSS)

References: (a) NISPOM, Chapter 8
(b) DCID 6/3

This Memorandum of Understanding (MOU) between the National Geospatial-Intelligence Agency (NGA) and the Defense Security Service (DSS), Designated Approval Authority for Applied Research Laboratories: University of Texas (ARL:UT), is for the purpose of establishing a secure communications link between NGA and ARL:UT for the electronic transfer of classified information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this MOU and Interconnection Service Agreement for the Interconnection of the NGA MSN and ARL:UT MSN IS, dated 29 AUG 06, summarize the information system (IS) security requirements for approval purposes and supplements ARL:UT approved system security plan (SSP).

1. Contract Information

This MOU describes the classified network arrangement between ARL:UT and NGA in support of the Monitor Station Network (MSN). The ARL MSN IS are government furnished equipment, sponsored by NGA, used to support the Global Positioning System mission of NGA. The contract number is N00024-01-D-6660. The prime contractor is ARL:UT, whose Cage Code is 55254.

The following ARL:UT key points of contact are identified:

NAME / TITLE / PHONE
Neil Fox / Field Security Officer (FSO) / 512-835-3365
Richard Mach / Project Manager/Information System Security Officer (ISSO) / 512-835-3614
Lorenzo Lopez / Information Systems Security Manager (ISSM) / 512-835-3755

At NGA direction, ARL:UT is establishing a remote access capability to the NGA MSN and the ARL MSN IS. The remote access to the NGA MSN is from ARL:UT-Austin. This capability will allow ARL:UT and NGA user personnel to access the NGA MSN and the ARL MSN IS as remote users.

The following NGA MSN key points of contact are identified:

NAME / TITLE / PHONE
Richard Cloninger / Information System Security Representative (ISSR) / (314) 263-4726
Lois Debrobander / Information Systems Security Manager / (314) 263-4182
Keith Ellis / MSN Program Manager / (314) 263-4149

5. Approval

The secure communication link between ARL:UT and NGA shall not be initialized until approval of these procedures by DSS is indicated below.

Defense Security Service

BOYLESTON.CLEM.O.1284706346

Clem Boyleston, Assistant Deputy Director
Office of the Designated Approving Authority
Defense Security Service
703.325.9453

National Geospatial-Intelligence Agency (NGA)

Thomas M. Shea COL, USA Ret.
Director, Office of GEOINT Sciences (SN)
Source Assessment & Foundation Group
National Geospatial-Intelligence Agency
314-263-4012

- **Questions**