CHAPTER 6 – PART 4
Firewall Technical Security Standards

1 BACKGROUND

The emerging need to connect the Department of Agriculture network to other government agencies, private companies and other organizations using Internet Protocol (IP) demands a coordinated and uniform approach to implementing secure IP connectivity. A characteristic of an interconnected environment is the ability to easily share resources and information. From a business perspective, this is a desirable feature, with hidden threats. Unfortunately the inherent nature of an interconnected architecture also results in sharing risks. A risk to one system becomes a risk to all systems.

In the past few years, government, private industry and academia have produced a body of security techniques, practices and tools to reduce the risks associated with inter-connectivity of networks. This document synthesizes this material to provide standards for Department of Agriculture agencies throughout the full life cycle process of procuring, implementing and operating firewall solutions and other perimeter protection for the USDA Enterprise Architecture.

Defense-in-depth refers to a layered architecture that provides increasing levels of protection for the USDA Enterprise Architecture. There are three layers in which security products can protect servers in this strategy: the network, the application and the kernel layers. In an ideal environment, there are one or more security services that protect each of these layers. Network firewalls and Intrusion Detection Systems (IDS) are the most common types of security products that work at the network layer. At USDA, the security objective is to ensure that the network perimeters, the DMZ, and the USDA Intranet are properly protected. Security functionality within the network perimeter and DMZ will also provide for the screening of all incoming traffic.
Three vital components of this defense strategy are system hardening; minimum system services and configuration

management practices sufficient to ensure that systems are patched as appropriate.

System hardening is the use of systems and system configurations that are in compliance with the USDA C2 level of security (based on the NSA Trusted Computer Security Evaluation Criteria) for all USDA IT Systems. System hardening, or C2, as defined by the NSA, includes making specific modifications to an operating system before it is put into use in order to aid in the reduction of operating risks and to increase system availability, confidentiality and integrity. The NSA C2 criteria, upon which the USDA C2 is based, requires individual user identification, user authentication, object reuse and auditing of system and user objects and processes.

Securing a system involves implementing a set of procedures, practices, and technologies to protect the information technology (IT) infrastructure as well as software and associated data throughout the organization. Minimum system services deployment is the use of only those TCP/IP services that are necessary to support the business function (for example, web servers should not also provide DNS services). The nature of evolving technology and the discovery of system software defects and TCP/IP vulnerabilities demand that information systems are patched to counter defects and to protect against known security vulnerabilities and system exploits.

Because computer security involves the enterprise's total set of exposures, from the local workstation or server to the Internet and beyond, it cannot be attained by simply implementing a "magic bullet" software product solution or by installing various security solutions. Computer security must be implemented by reliable mechanisms that perform security-related tasks at each of levels in the environment discussed above. Securing computer resources, applications, and related data is an integral part of securing an enterprise and hardening is the cornerstone of that model. More information on this subject can be obtained from NIST, 800-41.

2 POLICY

All agencies, mission areas and staff offices shall have a firewall installed and operating according to USDA policies between their networks and the USDA backbone network. All USDA agencies and mission areas will implement secure Internet Protocol (IP) connectivity from the Internet to Department of Agriculture networks, including all intranets and extranets, and provide minimum technical security standards for use in the selection and implementation approved firewalls and perimeter protection. In addition, all agencies must use USDA Application Internet Access Nodes.

This policy applies to the USDA perimeter or Demilitarized Zone (DMZ) between the Internet and USDA internal networks. The term DMZ is defined above and is widely used to describe the perimeter line of defense provided by firewalls to separate and protect internal networks from the global network community.

Policy Exception Requirements – There are no exceptions to the requirement to have firewalls. Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation time; exceptions will not be granted to the requirement to conform to this policy. The process for requesting Firewall Changes is covered in Section 3, Item K. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with an updated timeline for completion. CS will monitor all approved exceptions. This package will include the following:

a Business case necessitating the need for the exception and an explanation is requested;
b Details explaining how the confidentiality, integrity and availability of the sensitive information will be preserved [CS does not need to know if an agency/mission area is providing firewall or gateway to support to another entity

as long as the confidentiality, integrity and availability of sensitive information is maintained];

c Any associated costs for an alternative approach funded by the proposing agency;

d Assurances that any alternatives implemented will not adversely affect the costs, security, maintenance or operations of existing solutions implemented by other Departmental entities; and

e A schedule and tasks necessary to become compliant.

Any alternatives implemented will be subject to periodic reviews and must be adjusted, as necessary, to conform to the USDA Enterprise Architecture and Security standards. Waiver packages will be forwarded to the Associate CIO for Information Resources Management (IRM) in accordance with normal procedures. These packages will be forwarded to CS for review and further action.

3 PROCEDURES

The ultimate goal of this policy is to begin establishing a "Defense in Depth" Strategy for all USDA IT systems, networks, servers and applications in USDA. It is the policy of the Department of Agriculture that any direct connection of Agriculture networks to or from the Internet or Extranet must go through approved USDA firewalls. DMZ networks will be used where feasible to provide protection of USDA IT resources and to reduce exposure to outside attacks. A sample diagram that illustrates the typical DMZ concept is shown in Figure 1 below.

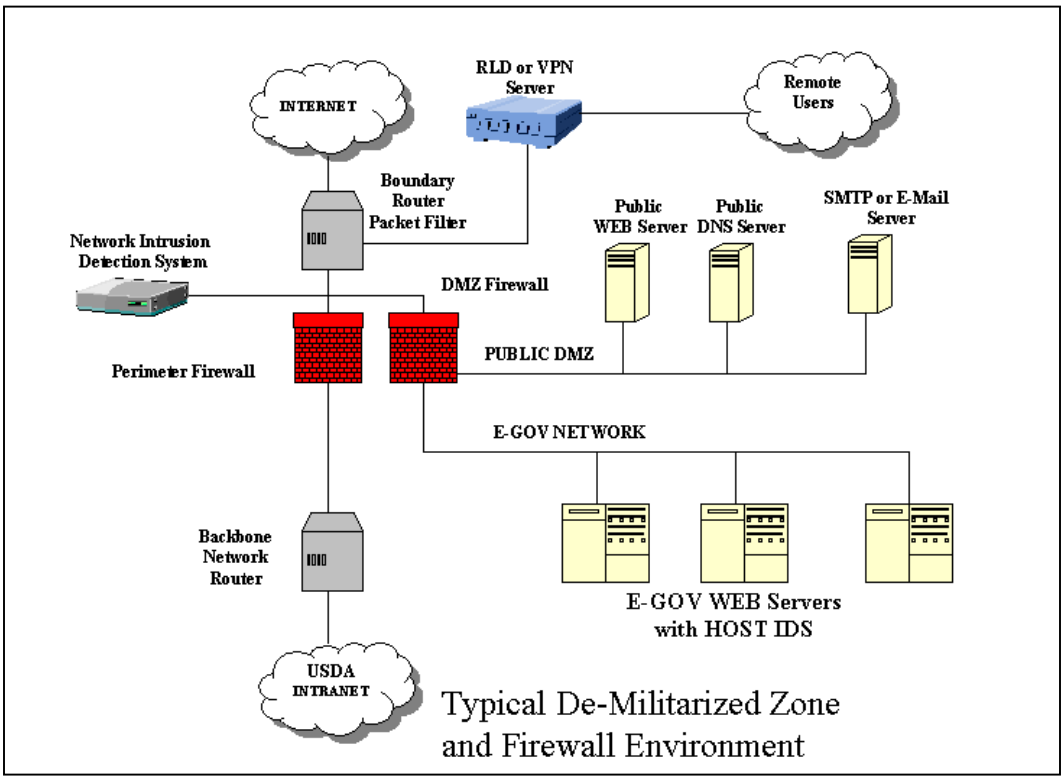

Figure 1

Dial-up connections and remote access will be centrally managed by each agency/ mission area to ensure integrity of network security. No remote non-centralized connections will be authorized. Approved authentication procedures for remote users must be established and the dial-up and/or remote service must be located at the outermost perimeter of the USDA DMZ. Host-based firewalls can also be used as an additional layer of agency security protection as suggested by the Defense-in-Depth strategy. All changes to approved firewall security configurations will be reviewed by the agency Configuration Control Board (CCB) and approved by the agency Designated Approval Authority (DAA) or Chief Information Officer. Approved firewalls will be configured to allow transmission of only USDA approved protocols that use Transmission Control Protocol/Internet Protocol (TCP/IP) stack (suite).

a Firewall Standards: This section defines the minimum technical security standards to be followed when implementing IP connections in conformance with DR-

3300-1 of the Telecommunications & Internet Services and Use Directive. This directive can be found at web site http://www.ocio.usda.gov/directives/index.html. This policy does not recommend or specify specific hardware or software products.

b Boundary Routers. Boundary routers and perimeter firewalls are to be used as part of the USDA or authorized agency perimeter protection. Boundary routers will function as the network perimeter interface and accept traffic from the Internet Service Provider. Due to their speed and flexibility, USDA or agency boundary routers will be used to filter unapproved protocols and pass traffic to the firewall to supply additional packet filtering processing. All boundary routers will also implement ingress and egress filtering to protect against IP address spoofing and directed IP broadcasts. In addition, boundary routers will provide the first level of network access control using router access control lists (ACL) according to this policy. Boundary routers and perimeter firewalls have the capability to filter based on TCP and UDP ports as well as IP addresses and incoming network interfaces.

c Perimeter Firewalls. A system designed to prevent unauthorized access to or from a private network. Perimeter firewalls protect USDA sites from exploitation of inherent vulnerabilities. These firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. Perimeter firewalls will use stateful inspection technology, unless a waiver has been approved.

d Services. Only services that are required and approved shall be activated. Any service that is not needed shall be turned off or deactivated. Any services that are permitted to pass through a firewall whether inbound or outbound shall be documented as to: 1) service allowed (including TCP or UDP port number), 2) description of the service, 3) business case necessitating the service, 4) internal management and security controls associated with the

service, 5) System Interconnect Agreements and Service Level Agreements, as applicable.

e Ingress Filtering. As defined in this policy, ingress filtering will be performed to exclude/reject all data packets that have an internal host address (i.e. source address is in the local domain). Non-routable IP addresses specified in RFC 1918 (Private Network Addresses) shall be dropped.

f Egress Filtering. Egress filtering will be performed to prohibit packets from leaving the USDA network that have non-USDA addresses as their source address.

g Inbound Services. Inbound services are prohibited, unless a valid business case can establish their validity. For SBU information, inbound services must provide authentication using one-time or session passwords, challenge and response protocols, digital signatures and/or encryption.

h Application Gateways. Application gateways will be used as a firewall component to protect client/server applications where the client or server resides on an external network. This provision may be waived for non-standard applications where a proxy application is not available or if the application provides user-to-user encryption.

i Audit Logs. All firewall systems will have an audit capability to monitor firewall operation and substantiate investigations of real or perceived violations of local security policies. At a minimum, the audit logs will track information on client transactions (i.e. IP address of source and destination, date and time, port, Uniform Resource Locator, etc), attempted access to network services, rejected source routed addresses, Internet Control Message Protocol (ICMP) redirects, and any system information the local security officer deems relevant. Archived audit logs will be maintained for a minimum of three years and kept as a separate backup for easy retrieval when needed.

USDA perimeter protection will have the capacity to identify each IP address to a workstation. For accountability reasons, adequate logging will be enabled at DHCP and Proxy servers (or any where internal and external addressing is used) to clearly identify the IP address and location of each workstation. In addition, all agency perimeter protection should be able to provide security alerts in various levels of severity. For high security alerts, the perimeter protection (firewall or IDS) should be able to send an E-mail or pager notification (or other real-time notification) to the System/Network Administrator (SA/NA) or Information Systems Security Program Manager (ISSPM) for immediate attention.

j Load Balancing/High Availability. If firewalls are implemented on sensitive systems, each agency should strongly consider the need for load balancing/high availability based on a system analysis and risk assessment. USDA firewalls that support sensitive or Mission Critical Systems will provide redundancy, dynamic load sharing and fail-over protection against hardware and software failures. These measures should enhance the department's network security posture and provide increased resource utilization, reliability and efficiency. Use of load balancing should be documented in the agency Disaster Recovery and Continuity of Operations Plans (COOP).

k Firewall Protocols. The sections below define allowed protocols:

Approved protocols (Agency Security Plans and Internal Operating Procedures must specify how each protocol will be securely operated)

FTP SMTP HTTP HTTPS DNS POP3S Secure FTP SFTP SSH NTP (outbound only) IMAPS

NOTE: These protocols must be run on well-known ports. Port reassignments are not permitted.

Approval to use other protocols will not be granted unless it can be demonstrated that the selected firewall configuration provides adequate security. If any of these protocols are already in use, a waiver must be obtained for their continued use. All inbound traffic not under the control of USDA must have a System Interconnect Agreement in place for all exception requests.

Requests for firewall changes will be sent from the agency or staff office to the TSO. The Firewall Configuration Control Board (CCB) will then make a determination on how to adjudicate the request on a case-by-case basis. In order to be approved, the CCB must reach a consensus approval. If the CCB has approved the change, the TSO will convey the decision to the firewall operation contacts for implementation and to the requesting agency.

l Sensitive But Unclassified (SBU) Data. The user or service provider will encrypt all sensitive information prior to transmission over any public or government owned/furnished network. Applications that use the Internet or other public networks for the transmission of SBU information will use Virtual Private Network (VPN) circuits, application level encryption, or other approved gateways as a means to protect data.

m Firewall User Accounts. All externally addressable host systems must have their own Security Plan and be accredited/certified in accordance with Annual Plan Guidance, CS-002. Firewall systems will operate only with those services required to function as a firewall. Because of the limited number of firewall network interfaces, firewalls will deploy static routing only to reduce the number of routing decisions imposed by dynamic routing protocols. All user accounts must be implemented in a secure manner.

n Internet Services. All Internet and other public access network servers will be located at the USDA network DMZ. No web servers accessible to the public will be placed inside the USDA Intranet. These servers shall be protected

by firewalls on the public side of the USDA network and will include their own intrusion detection systems.

Internet servers that currently operate inside the USDA network firewall perimeter need to obtain an exception. Include in this waiver request a plan to migrate the server to the public side of the USDA network. These servers shall be readdressed with IP addresses that make them clearly and easily distinguished by other internal security perimeters. All Internet and other public access network servers shall be registered with the Associate Chief Information Officer.

o Firewall Consoles. All firewall consoles will be located in a physically secure area and require a logical security level equal or exceeding C2 security functionality. C2 security is the minimum security rating for computing products; it requires the system to have discretionary resource protection and auditing capability. Only designated administrator accounts will be installed on a firewall. Management consoles must provide a secure (encrypted) communications path between the management console and the firewall being managed.

p Monitoring. The firewall system shall provide for a monitoring capability. This capability can be provided as an integral part of the firewall by the provider or by the addition of a third party product. The monitoring product must provide remote notification capability.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Provide technical standards for firewalls used in USDA's Information Technology environment;

(2) Promptly review for approval requests for exceptions to this policy and provide a response to the agency/mission area;

(3) Conduct reviews to ensure compliance by USDA agencies with this policy by auditing firewalls standards;

(4) In coordination with TSO, the registration authority, maintains a listing of all registered WWW servers and public access servers within the department;

(5) Coordinate with agencies/mission areas to promote and effect the Defense in Depth environment within USDA; and

(6) Periodically review and update this policy and procedures as required;

b Agency Management and Information Technology Officials or Chief Information Officer will:

(1) Ensure the provisions of this policy are implemented in all agency/mission area IT environments;

(2) Make certain that dial-up connectivity is centrally managed and users of dial-up services are fully authenticated;

(3) Make sure that all relevant agency personnel are acquainted with the provisions of this policy and procedures with a focus on the Information Systems Security Program Manager and System/Network Administrators (SA/NA);

(4) Make certain that all agency security plans and internal operating procedures include instructions for the secure use of approved firewall protocols;

(5) Ensure that any changes made to firewall and gateway standards undergo review by the agency Configuration Control Board (CCB) and are

approved by the Designated Approval Authority (DAA);

(6) Make certain that agency personnel promptly respond to security alerts from firewalls;

(7) Prepare formal exception requests for firewalls that do not meet the requirements of this policy in conformance with the policy exception section above; actively work to achieve conformance; exception requests will be signed by the Agency Head/CIO and will be forwarded to OCIO; and

(8) Actively participate with the Associate CIO for CS to establish a Defense-in-Depth strategy to protect all of USDA's IT assets.

c <u>The agency Information Systems Security Program Managers(ISSPM) will:</u>

(1) In coordination with the agency SA/NA will ensure that all agency firewalls comply with this policy and standards;

(2) Include the requirements of this policy in agency security plans and internal operating procedures to ensure secure use of approved firewall protocols and standards;

(3) Participate, via the agency CCB, in the review of changes to firewalls standards;

(4) In conjunction with the agency SA/NA, ensure that all remote connections are centrally managed and users of remote services are fully authenticated;

(5) In coordination with the agency SA/NA, respond promptly to high security alert notifications from firewalls taking appropriate remedial action to protect USDA information assets;

(6) Conduct periodic reviews of all firewall and gateways to determine compliance with protocols and standards; report any non-compliant firewalls to the Agency Head/CIO; actively work to remedy non-compliance; and

(7) Participate in the preparation of waiver packages, as required.

d Agency System/Network Administrators will:

(1) Ensure that agency firewalls comply with this policy and standards;

(2) Include these standards and approved protocols in internal operating procedures for firewalls;

(3) Participate in the central management of all agency remote connections ensuring that users of dial-up services are fully authenticated;

(4) Promptly respond to high security alert notifications from agency firewalls and in coordination with the ISSPM take appropriate remedial action to protect USDA information assets; and

(5) Review all agency firewalls standards and protocols to ensure that they comply with this policy; actively participate in the preparation of exception packages, as required.

- END -