

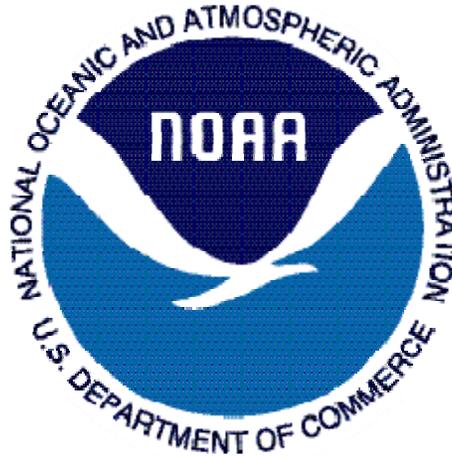
NOAAnet USER CONNECTION AGREEMENT

Between National Oceanic and Atmospheric Administration (NOAA)
The National Weather Service (NWS)

NOAAnet
NOAA8204

And

NOAAnet Data Customer



October 7th, 2009

<p>NOAA NWS CIO 1325 East-West Highway, Room 17424 Silver Spring, MD 20910</p>	<p>NOAAnet Data Customer Name _____ NOAAnet Data CustomerAddress _____</p>
--	--

NOAAnet USER CONNECTION AGREEMENT

SECTION 1 – SUPERSEDES

None

SECTION 2 – INTRODUCTION

This NOAAnet User Connection Agreement (NUCA) authorizes and documents the understandings, roles and responsibilities between NOAA's (National Oceanic and Atmospheric Administration) National Weather Service (NWS) Wide Area Network (WAN) NOAAnet (NOAA8204) and _____ *the User*. This agreement between National Oceanic Atmospheric Administration (NOAA)/NWS and User is established to facilitate the development, management, operation, and security of a connection between both parties. This agreement will govern the relationship between NWS and User, including designated managerial and technical staff, in the absence of a common management authority. This agreement is effective when signed by the NWS and User.

SECTION 3 – GENERAL DESCRIPTION

NWS NOAAnet (NOAA8204) is a general purpose shared network that provides a secure, private WAN backbone using Multiprotocol Label Switching (MPLS) services. The NOAAnet system consists of edge devices, Customer Edge (CE) routers and firewalls; the carrier provided WAN that connects those devices; a secure out of band subsystem used to access and manage remotes sites in case of a network outage; and the automated systems that manage and monitor traffic between the CE routers.

NOAAnet (NOAA 8204) has been designated as a High Impact system and implements the Security Controls required for a High Impact system based on High Availability requirements.

The information handled by the NWS NOAAnet (NOAA8204) has a moderate confidentiality categorization. The classification level of the information to be exchanged is unclassified.

There is no data exchanged in that the User does not transmit or receives any data from NOAAnet and no User data is stored within the boundaries of NOAAnet.

Data Services

NOAAnet (NOAA8204) provides firewall and virtual private network (VPN) management services via a high availability WAN access, if required that is used to connect various systems within the NWS and User. The purpose of these services is to facilitate the movement of data to and from various systems and the Internet as connected by NOAAnet.

The Gateway operates a cluster of servers that disseminate and receive data files containing meteorological data in predefined formats. The purpose of this connection is for data ingest and dissemination. In general, these information services (ingest) are characterized as follows:

- File Ingest using SCP, HTTP, and FTP
- Message Ingest, both Internet Protocol (IP) based and non IP using either the X.25 or asynchronous communications

Audit Trail Responsibilities

NOAAnet edge devices are configured to log all sessions and all unsuccessful access attempts. Logs are compressed and archived on a monthly basis. Archives are maintained for one year. Logs include event type, date and time. NWS NOAAnet (NOAA8204) does not require audit information from the User, and will not access audit information across the connection.

SECTION 4 – COMMUNICATIONS

Frequent formal communications are essential to ensure the successful management and operation of the connection. The NWS and User agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in writing unless otherwise noted.

NWS and the User agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct contacts between technical leads to support the management and operation of the connection. To safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, NWS and User agree to provide notice of specific events within the time frames indicated below:

User Community

NWS NOAAnet (NOAA8204) data and products form a national information database and infrastructure which can be used by other governmental agencies, the private sector, the public, and the global community.

Information Exchange Security

All NOAAnet system boundaries are monitored and protected by stateful firewalls. As a standard, NOAAnet enforces stateful firewall services on all centrally managed CE devices for all sessions. The firewall will permit access based on:

1. Source IP address
2. Destination IP address
3. Protocol (TCP/UDP)
4. Port(s)

The NWS does additional security utilizing host-based firewall policies. NOAAnet (NOAA8204) does not encrypt customer data traversing the network; however all access, either network based or via out of band (dial up) access to NOAAnet edge devices requires RSA two factor authentication and is encrypted in accordance with FIPS140-2.

Trusted Behavior Expectations

The following section outlines expectations regarding Rules of Behavior (ROB) to be followed by the NWS NOAAnet (NOAA8204) and User to protect information exposed to this connection. NWS reserves the right to terminate this agreement if the User fails to comply with these expectations.

- NOAA employees and contractors agree to conform to the guidelines in accordance with NOAA ROB.
- NWS NOAAnet (NOAA8204) expects that the User will follow Notification and Escalation Procedures outlined in this document.
- NWS NOAAnet (NOAA8204) expects that the User will take appropriate measures to prevent operational attacks, such as denial of service.

Security Parameters

Access to NOAA network resources and systems via the NOAAnet backbone are controlled through NOAAnet stateful firewall services at every edge and authenticated based on both protocols and ports. NOAAnet provides and manages VPN and firewall connections as required to help ensure secure data transfer between NWS systems and User. All firewall changes are submitted to the NOAAnet Change Control Board (CCB) for review and approval prior to implementation.

Material Changes to System Configuration

Planned technical changes to the system architecture as it relates to the connection will be reported to

technical staff before such changes are implemented. The NWS agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign the NUCA within one (1) month of implementation.

New Connections

This NUCA does NOT authorize establishment of new connections to NOAAnet or with any other IT system, including systems that are owned and operated by third parties.

Personnel Changes

The NWS and User agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, both parties will provide notification of any changes in point of contact information.

Notification and Escalation Procedures

In the event of service outage or service degradation Users should notify the NOAAnet NOC at 1.888.NOAANET (1.888.662.2638) or email noaanet.support@noaa.gov. All NOAAnet Users are required to provide email and telephone contact information for both outages and security incidents as part of the Signature page.

Training and Awareness

All NOAA personnel and contractors are required to successfully complete the security awareness training prior to authorize access granted to NOAA/NWS information systems, when required by system changes, and at least annually thereafter. The User may be granted temporary access where an information system security orientation is provided with granted access, until the training requirement is met. In this instance, training shall be met within thirty (30) calendar days. If the User refused to engage in, or cannot meet the training requirement due to extenuating circumstances, access to information and resources must be suspended.

All security training is identified by the Information Technology System Officer; progress is tracked in the NOAA IT Security Awareness training system and reported to the NOAA IT Security Office and the NOAA Chief Information Officer (CIO).

Security Training and Awareness is not required for User community.

SECTION 5- SERVICES

NOAAnet (NOAA8204) services include:

- Network design solution development,
- Acquisition services for hardware and telecommunication services,
- Logistics management, which includes the ordering, installation coordination, and the ongoing management of telecommunications carrier services,
- Asset and configuration management of all NOAAnet managed infrastructure devices,
- Service assurance including incident management and problem management, and
- Performance management

Operational Security Mode

Federal Information Processing Standard (FIPS) 199 defines the security categories, security objectives for confidentiality, integrity, and availability, and impact levels of low, moderate, and high. Selection of NOAAnet (NOAA8204) security category is based on mission and:

- Loss of confidentiality (unauthorized disclosure)
- Loss of integrity (unauthorized modification or destruction)
- Loss availability (disruption of access to or use)

The NOAAnet (NOAA8204) Security Categorization (SC) has been determined using the guidance of FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60. The process and analysis are documented in the NOAAnet (NOAA8204) FIPS 199 SC as such NWS NOAAnet (NOAA8204) supports the following SC for Confidentiality, Integrity, and Availability for data transmitted across this connection:

SC NOAA8204 = {(confidentiality, Moderate), (integrity, Moderate), (availability, High)}

Information System Impact Level (for selecting baseline controls): **HIGH-Impact**

- Confidentiality – Moderate
- Integrity – Moderate
- Availability – High

Specific Equipment Restrictions

The User Community connecting to the NWS NOAAnet WAN should be able to connect via Ethernet or fiber.

Security Documentation

The NWS and NOAAnet operate in accordance with System Security Plans that satisfy the requirements outlined in NIST SP 800-53 rev 2. The NWS operates NOAAnet (NOAA8204) following NIST security guidelines for Certification and Accreditation (C&A). The NOAAnet C&A is covered under NOAA8204 which has received its Authority to Operate (ATO) in December 2008.

SECTION 6 – RESPONSIBILITIES

NOAA's NWS Office of the CIO Responsibilities

NWS is responsible for operational support and configuration management of all NOAAnet provided equipment and peripheral devices. This includes hardware and software management, router configurations, firewall configurations, overall system configurations, and vendor support coordination.

NOAAnet User Community Responsibilities

The NOAAnet User Community is responsible for providing to NOAAnet the point of contact information for all sites to support the implementation and operational requirements of the NOAAnet service. This includes but is not limited to, network event notifications that may impact service and have security implications.

SECTION 7 – FORMAL SECURITY POLICY

NWS NOAAnet (NOAA8204) is governed by the information security policies of the United States Federal Government, including OMB, DOC and NOAA. For details, refer to NOAAnet SSP v1.4 dated December 8, 2008 page 24.

SECTION 8 - DISASTERS AND OTHER CONTINGENCIES

In the event of a disaster, the NWS will follow the NOAAnet Contingency Plan (CP). This plan establishes procedures to recover the information system following a disruption. The following objectives have been established for this plan:

- Identify the following phases:
 - Notification/Activation: detect and assess damage and to activate the plan.
 - Restoration: provide temporary IT operations and/or recover damage done to the original system to a level that can support the User's system and processes.
 - Reconstitution: restore the User to normal operations.

- Identify the activities, resources, and procedures needed to carry out identified system requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated NWS personnel and contractors provide guidance for recovering the User's system during prolonged periods of interruption to normal operations.
- Ensure coordination with other NWS staff, and external points of contact who will participate in the contingency planning strategies.

SECTION 9 – SYSTEM BOUNDARIES AND PHYSICAL LAYOUT

The NWS Office of the CIO is responsible for support and asset management associated with the CE router and any associated equipment used for performance measurement and out of band communications, including probes and modems. All sites are furnished through direct access solution to the NOAA net backbone. All activity, ingress/egress, is captured via CE router audit logs.

SECTION 10 – MODIFICATION, TERMINATION, AND OTHER CONDITIONS

The NUCA may be modified by NWS upon reasonable notice to User. The NWS or User may terminate its participation in the NUCA with written notice to the other 30 days prior to such withdrawal. Nothing in the NUCA alters the statutory authorities and responsibilities of the NWS or User. It is intended to facilitate those authorities through cooperative action. In the event of a security incident, this NUCA may be terminated by NWS without reasonable notice to User.

SECTION 11 – TERMS OF AGREEMENT

This NUCA will remain in effect for a five (5) year period after the last date on either signature block below. After five (5) years, this agreement will expire without further action. If the NWS and User wish to extend this NUCA, they may do so by reviewing, updating if necessary, and reauthorizing this NUCA. The newly signed NUCA should explicitly supersede this NUCA, which is referenced by title and date.

SECTION 12 – TOPOLOGICAL DRAWING

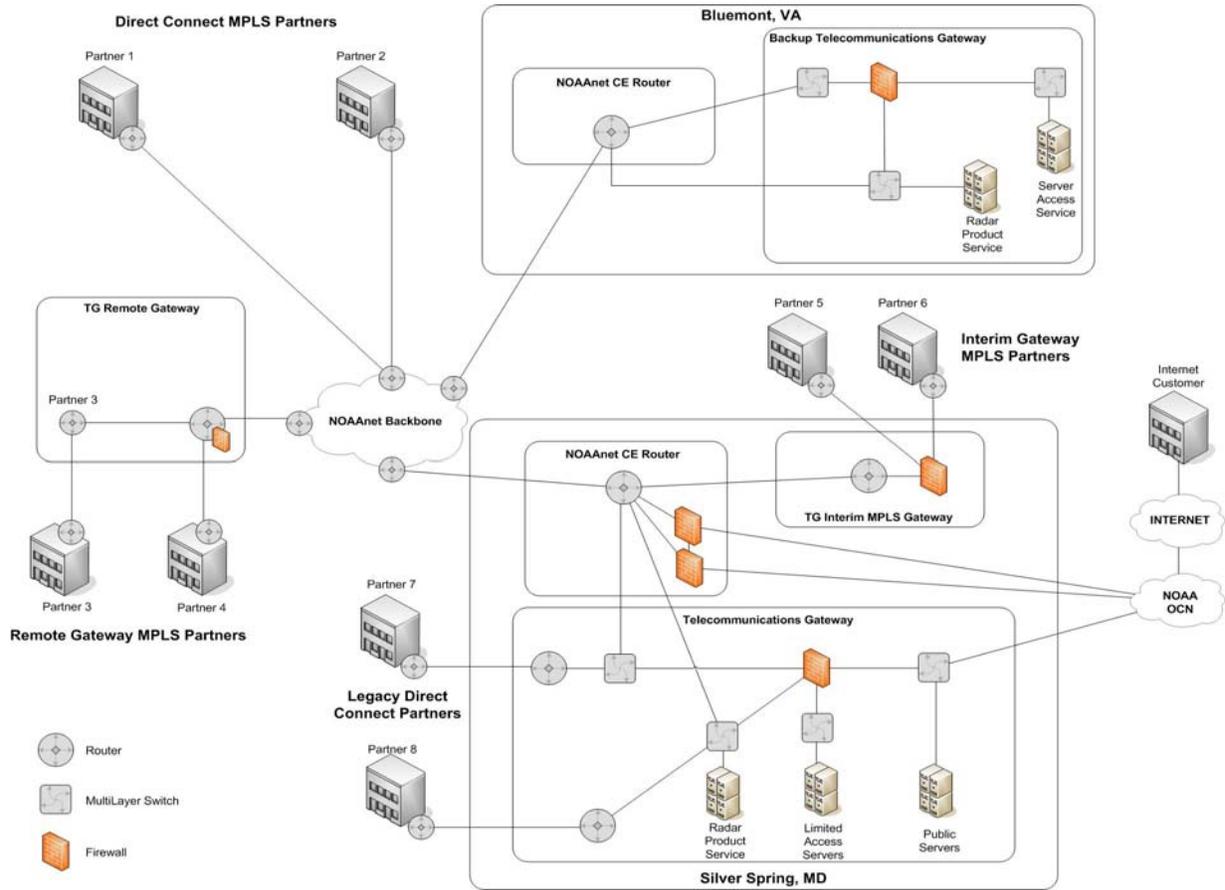


Figure1. NWS and Other Entity Interconnect Diagram

SECTION 13 – SIGNATORY AUTHORITY

I agree to the terms of this User Connection Agreement.

NOAA/NWS	NOAAnet Data Customer _____
Name: Craig Hegemann	Name:
Title: NOAAnet System Owner	Title:
Signature:	Signature:
Date:	Date:

APPENDIX A: Physical and Environmental Controls (Recommendations)

PHYSICAL ACCESS CONTROL

The User should provide controls to all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. The User should control physical access to NOAAnet equipment independent of the physical access controls for the facility.

ACCESS CONTROL FOR TRANSMISSION MEDIUM

Physical protections applied to NOAAnet distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

MONITORING PHYSICAL ACCESS

The User should monitor physical access to information systems to detect and respond to security incidents. The User should monitor real-time intrusion alarms and surveillance equipment.

VISITOR CONTROL

The User should control physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible. The User should escort visitors and monitors visitor activity, when required.

ACCESS RECORDS

The User should maintain visitor access records to the facility where the NOAAnet equipment resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records.

The User should employ automated mechanisms to facilitate the maintenance and review of access records. The User should maintain a record of all physical access, both visitor and authorized.

POWER EQUIPMENT AND POWER CABLING

The User should protect power equipment and power cabling for NOAAnet equipment from damage and destruction. The User should employ redundant and parallel power cabling paths.

EMERGENCY SHUTOFF

The User should provide, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment. The User should protect the emergency power-off capability from accidental or unauthorized activation.

EMERGENCY POWER

The User should provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. The User should provide a self-contained, long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

FIRE PROTECTION

The User should employ and maintains fire suppression and detection devices/systems that can be activated in the event of a fire. The User should employ fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.

TEMPERATURE AND HUMIDITY CONTROLS

The User should regularly maintain, within acceptable levels, and monitors the temperature and humidity within facilities containing NOAAnet equipment.

WATER DAMAGE PROTECTION

The User should protect the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel. The User should employ mechanisms that, without the need for manual intervention, protect NOAAnet equipment from water damage in the event of a significant water leak.

DELIVERY AND REMOVAL

The User should control information system-related items entering and exiting the facility and maintains appropriate records of those items.

LOCATION OF INFORMATION SYSTEM COMPONENTS

The User should position NOAAnet components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.