*Sample Access Control Plan- The purpose of this text is NOT to dictate a certain format or content, but to show one simple way of fulfilling the requirement to prepare access control plans that identify measures and procedures and demonstrate compliance.*

# NOAA X Laboratory/Center/Office etc.

NOAA's X Laboratory/Center/Office at [address] has controlled technology that is EAR 99 and controlled technology with specific ECCNs. Access controls for EAR 99 technology are listed on the first page of this plan. Access controls for other controlled technology is listed on subsequent pages.

……..

**This facility does not maintain a written list of EAR 99 technology. For all EAR 99 technology, access is controlled by prohibiting persons within the following categories from entering NOAA X Lab/Center/Office:

1. Foreign nationals from Cuba (*See*, 15 CFR 746.2 for licensing requirements)
2. Foreign nationals from Iran (S*ee*, 15 CFR 746.7 for licensing requirements)
3. Foreign nationals covered under the "Entities List" (Published at 15 CFR 744, Supp. 4 and at http://www.bis.doc.gov/Entities/Default.htm)

For all other foreign nationals, EAR 99 technology may be released without a license, unless you know that the foreign national intends to use such technology in activities related to nuclear, chemical or biological weapons or missiles. *See*, 15 CFR 744.

In the event that NOAA X Laboratory/Center/Office, etc… decides to allow a foreign national in categories 1-3, above into its facility, steps will be taken to ensure that the foreign national does not have access to ***EAR-controlled technology*** unless a license is in place or it has been determined that no license is required. Given the likelihood that a license would be required, the facility must consult with their Line Office/Corporate Office Controlled Technology Coordinators before asserting that no license is required for individuals from categories 2 and 3. Releases of EAR 99 technology to Cuban nationals ALWAYS require a deemed export license.

In cases where a license is required to access controlled technology, a license must be obtained prior to the visit.

The access control sheets for all other technologies follow this coversheet.

Date:

Submitted by:

Location:

For all technology controlled for Anti-Terrorism (AT) reasons only (See, 15 CFR Part 742.8-742.10 and 742.19), this facility controls access by prohibiting persons from the following countries from entering:

1. Foreign Nationals from North Korea (*See*, 15 CFR 742.19 for licensing requirements)
2. Foreign Nationals from Sudan (*See*, 15 CFR 742.10 for licensing requirements)
3. Foreign Nationals from Syria (*See*, 15 CFR 742.9 for licensing requirements
4. Foreign nationals from Cuba (*See*, 15 CFR 746.2 for licensing requirements)*
5. Foreign nationals from Iran (*See*, 15 CFR 742.8 for licensing requirements) *

In the event that X Laboratory/Center/Office, decides to allow a foreign national in categories 1-5 into its facility, steps will be taken to ensure that the foreign national does not have access to EAR-controlled technology unless a license is in place or it has been determined that no license is required. Given the likelihood that a license would be required, the facility must consult with the Line Office/Corporate Office Controlled Technology Coordinators before asserting that no license is required for individuals from categories 1-5.

**See*, Page 1 for EAR 99 controls related this group of foreign nationals.

## Access Control Information Sheet
## NOAAXXX

**Date:** December 2, 2005

**Item Name (and ECCN):** SGI Altix 3700, Altix 3800, Origin 3900 clusters - 4E001 (sunflower codes – CD000011111), CD0000111112, CD0000111113, CD0000111114)

**Responsible Individual/Title:** Jane Smith/ Senior IT Manager

**Location(s):** Computer Room, Department of Commerce Building, Any Street US, Anytown USA.

**Organization (Laboratory or Program):** NOAA Lab/Center Office X

**Description and relevant performance metrics:** Digital Computers with 2688 Intel Itanium Processors and 384 MIPS Processors distributed amongst 10 single image NUMA-based clusters. Individual clusters have a compute capability in excess of 190 million MTOPS

**EAR Controls and Restrictions:** NS, MT, CC, AT, NP, XP (*Described in 15 CFR Supplement No. 1 to part 740 country groups)*

**Authorized Access:**

**Physical:**

1) Only authorized personnel are allowed unescorted access to the Computer Room.
2) Prior to a tour, Operations conducts a sweep of the room to ensure no technology is visible.
3) All guest workers are escorted.

**Logical Access:**

1) Only authorized accounts are allowed remote access to the interactive hosts of the HPC. There are two groups of accounts: **administrators** – those with privileged access, and **users** – those with non-privileged access, or "mere-use" access.
2) "Authorized accounts" are accounts that have met the necessary requirements as determined by the system owner. All accounts are reviewed routinely to ensure appropriate levels of access are maintained.
3) All levels of access require authentication and all passwords are maintained to the NOAA Password Policy requirements.

**Physical Security:**

1) There are three entrances to the computer room. Two entrances are controlled by RFID badges. The third is secured by a cipher lock.
2) All points of entrance are under video surveillance, monitored by …..24x7.
3) The System Owner and COTR approve all access to the computer room.
4) The Computer Room is monitored by the Operation staff 24x7.

**Continuity of Service and Operations:**

The security of this equipment is not impacted by power failure.

**Technical:**

Users only have access to publicly available source code.

**Awareness and Training:**

1) All operators have been briefed by the Administrative Officer on the restrictions concerning export controls for this item.
2) All account holders are responsible for reviewing and agreeing to the rules of behavior, and for taking the annual Security Awareness Course.

**Reporting Violations:**

Individuals who think that export controls have been violated, whether deliberately or by accident, will report their concerns to the Lab/Center/Office Administrative Officer, to the System Security Officer, or to the Deputy Director, who will inform the Physical Security Officer.