GUIDANCE FOR CREATING ACCESS CONTROL PLANS

Background

Each National Oceanic and Atmospheric Administration (NOAA) facility must have an "Access Control Plan" that identifies all of the measures and procedures that have been implemented at that facility to control foreign nationals' access to technology that is regulated under the Export Administration Regulations (EAR), and that demonstrates that the facility has instituted sufficient measures and procedures to assure full compliance with the EAR. Every facility that has been assessed for EAR-controlled technology must create an Access Control plan that documents the findings of the controlled technology assessment. Even if there is no controlled technology at the facility, one must document that no controlled technology was found at the facility. If there is EAR-controlled technology at the facility, the Access Control plant must include the measures implemented to safeguard the technology

An Access Control Plan is not a one-size-fits-all document. Each facility must look at its particular circumstances and take appropriate steps to control access to EAR-controlled technology based on site-specific factors such as physical layout of the facility, locations of EAR-controlled technology within the facility, proximity of the facility to other parts of NOAA and other entities, security measures already in place or that will be put in place for reasons other than export control, duties and home country of foreign nationals working at the facility, and the frequency and home country of foreign national visitors at the facility.

The basic component of each facility's Access Control Plan is an "Access Control Information Sheet" for EAR-controlled technology. Each Access Control Information Sheet shall contain the information identified below and shall follow the format shown.

In most cases, EAR-controlled technology must have a separate Access Control Information Sheet that describes the procedures that prevent unauthorized access to the controlled technology.

ACCESS CONTROL INFORMATION SHEET

[Required Data]

- Date Access Control Information Sheet Prepared
- Item Name (and ECCN, if applicable)
- Organization
- Description
- Physical Location(s)
- EAR Controls and Restrictions
- Individuals Authorized Access to technology
- Physical/Electronic Security/Access Control Measures Implemented to Ensure Only Authorized Access Is Provided
- Where to Report Access Control Violations

It may be appropriate for the Access Control Plan to document controls on certain technology in some other way. For example, a facility containing only EAR-99 technology may choose to deny access to those foreign nationals whose access to EAR-99 technology is controlled under the EAR (such as foreign nationals from Cuba, Iran, and foreign nationals covered under the "Entities List," which is published at 15 CFR 744, Supp. 4 and at http://www.bis.doc.gov/Entities/Default.htm). If the Access Control Plan documents access controls for technology that ensures full EAR compliance, then individual Access Control Information Sheets are not required for the technology at that facility.

Summary: The Access Control Plan at each facility should address all measures and procedures in place to prevent access to controlled technology at that facility. There must be access controls documented for every entry identified on the controlled technology inventory, including EAR 99. The Access Control Plan must demonstrate that the facility has instituted sufficient measures and procedures to assure full compliance with the EAR; however, each facility has some flexibility to prepare its plan based on the particular circumstances at that facility.

NOTE: To comply with Office of Inspector General requirements, each Line Office or Corporate Office (LO/CO) must maintain Access Control Plans for each "facility," not for identical technology located at different facilities. The Office of the Chief Administrative Officer must collect plans from each LO/CO for each location. *See*, NOAA Administrative Order 207-12, Section 6.02)

The Analysis Tool below is intended to provide assistance in developing Access Control Plans.

Analysis Tool for Developing Access Control Plans:

1. Based on your equipment list, please attach a separate list identifying specific equipment for which foreign nationals have access to the associated technology or information regarding the design, development, production or "use" of the equipment. Do not include knowledge that can be obtained through public sources, for example, through the internet or other publicly available information).

2. Do foreign nationals:

   a. Have access to research, other than their assigned projects within your facility?

   b. Participate in several projects at one time within your facility?

   c. Share or integrate research which they conduct outside your laboratory?

3. If you have operating manuals which came with the equipment, are these generally limited to basic instructions for operation or do they provide details for the assembly

and disassembly of equipment within your facility? Did you obtain the manuals from publicly available sources or proprietary sources?

4. If the manuals were obtained from proprietary sources, please specify.

5. List other methods by which you receive technical data related to the equipment in your facility.

6. Does your research involve patents, or Cooperative and Research and Development Agreements (CRADA) with private companies or universities? If yes, please describe:

Note: Research could be subject to the EAR if it is conducted under CRADAs and other arrangements with non-disclosure agreements that place restrictions on the public dissemination of research results.

7. Do you have any electronic security measures at your facility which prevent foreign nationals from gaining access to controlled technology? If yes, please describe.

8. Do you have any physical security measures at your facility which prevent foreign nationals from gaining access to controlled technology? If yes, please describe.

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.