

ITAR/Export Control

Category: Security Policies

The PI must, by law, manage, protect and control the export of the project's data in a way that complies with the security category of the data. There are five categories of data:

- Mission Information (MSN)
- Business and Restricted Technology Information (BRT)
- Scientific, Engineering, and Research Information (SER)
- Administrative Information (ADM)
- Public Access Information (PUB)

WARNING: Mission Information requires the most stringent security control and protection. Currently, the NAS Facility is not configured to provide services for MSN data. For Business and Restricted Technology Information (which includes ITAR/Export Control Data), no world access (write/read/execute) is allowed.

Detailed descriptions of each data categories are as follows:

Mission Information (MSN)

If the information, software applications, or computer systems in this category are altered, destroyed, or unavailable, the impact on NASA could be catastrophic. The result could be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical Agency mission. Examples in this category are those that control or directly support one of the following:

1. Human space flight
2. Wide Area Networks
3. Development of the data or software used to control human flight
4. Training simulation vehicles
5. Wind tunnel operations
6. Launch operations
7. Space vehicle operations

Business and Restricted Technology Information (BRT)

This category consists of information that NASA is required by law to protect. It includes information, software applications, or computer systems that support the Agency's business and technological needs. In general, if information in this category should be disclosed inappropriately, the disclosure could result in damage to our employees, in loss of business

for our partners and customer businesses, in contract protest, or the illegal export of technology. This category includes systems containing technological information that is restricted from general public disclosure because of public laws. Examples in this category are those that are related to the following kinds of information:

1. Financial
2. Legal
3. Payroll
4. Personnel
5. Procurement
6. Source selection
7. Proprietary information entrusted to the Government
8. Export controlled technical information (includes disclosure to foreign nationals)

Scientific, Engineering, and Research Information (SER)

All official NASA information held by NASA employees may be released publicly only in accordance with NASA regulations; however, systems in this category do not contain information for which the release is otherwise governed by law. This category consists of information that supports basic research, engineering, and technology development but is less restricted against public disclosure.

1. Alteration, destruction, unauthorized disclosure, or unavailability of the systems, application, or information would have an adverse or severe impact on individual projects, scientists, or engineers; however, recovery would not impede the Agency in accomplishing a primary mission.
2. Integrity is the driving concern in this category followed by availability. Confidentiality is important and should be considered in a risk assessment insofar as it protects individual researchers from such things as premature disclosure of their work by another party. The impact, however, is primarily on an individual rather than on the Agency.

Administrative Information (ADM)

Administrative Information includes, but is not limited to electronic correspondence, briefing information, project/program status, infrastructure design details, predecisional notes, vulnerability descriptions, passwords, and internet protocol addresses. Organizations run various applications-from problem reports to configuration management tools-on administrative IT systems.

1. This category includes systems, applications, and information that support NASA's daily activities, such as electronic mail, forms processing, networking, and management reporting.

2. Integrity and availability are the driving IT security concerns. The impact is primarily managerial in nature, which would require time and resources to correct. Confidentiality may be of concern in certain specific administrative information. In such instances, additional security controls must be imposed as a risk analysis dictates.

Public Access Information (PUB)

This category includes information, software applications, and computer systems specifically intended for public use or disclosure, such as a public web site or hands-on demonstrations. The loss, alteration, or unavailability of information in this category would have little direct impact on NASA's missions but might expose the Agency to embarrassment, loss of credibility, or public ridicule.

1. Information posted for public access which could expose NASA missions to risk if compromised should be afforded additional protective measures. In these cases, the baseline requirements for ADM information should be implemented. (For example, contractors may submit proposals based on information from NASA web sites. Loss, alteration, or unavailability of data at the site could result in protests, thereby impacting procurement cycle time and ultimately NASA missions.)
2. Integrity and availability are the driving concerns. IT security controls are selected to protect the resources themselves and are not intended to protect the confidentiality of the information.

Article ID: 154

Last updated: 08 Aug, 2012

Policies -> Security Policies -> ITAR/Export Control

<http://www.nas.nasa.gov/hecc/support/kb/entry/154/?ajax=1>