

Cyber Threats and Their Targets

If you suspect your facility's technology or information has been targeted, report it to your FSO or security point of contact.

Cyber threats include, but are not limited to:

- Insiders
- Hackers
- Cyber Criminals
- Terrorists
- Organized Crime
- Foreign Intelligence Entities

Targets include, but are not limited to:

- Sensitive company documents and proprietary information
- Export controlled/classified information and technology
- Information on DoD-funded contracts
- Sensitive technological specification documents
- Users' login IDs and passwords
- Personal Identifying Information (SSN, date of birth, address)
- Contact rosters and phone directories
- Technology information, which includes both classified and unclassified
 - Militarily Critical Technology:
 - Any technology that would allow potential adversaries to make significant advances in the development, production, and use of military capabilities
 - Department of Defense maintains a list of applicable technology
 - Export is strictly controlled by the International Traffic in Arms Regulations (ITAR)
 - Illegal export of this technology often results in fines and/or criminal charges
 - Dual Use Technology:
 - Technology that has both military and commercial use
 - Export is strictly controlled and enforced under the Export Administration Regulations (EAR)
 - Illegal export of this technology often results in fines and/or criminal charges

- Examples of most targeted technologies in recent years:
 - Information systems
 - Aeronautics including technology related to unmanned aerial vehicles (UAVs)
 - Lasers and optics
 - Sensors
 - Marine systems
 - Positioning, navigation, and time
 - Electronics
 - Armaments and energetic materials
 - Materials and processing