



GUIDELINES AND STANDARDS FOR PHYSICAL SECURITY

ASTM F 1029, *Standard Guide for Selection of Physical Security Measures for a Facility*, ASTM International, 1997: Very basic introduction to establishing threat level and considering protection options.

DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, Director of Central Intelligence, 18 November 2002: Detailed requirements for spaces that will be certified to house particularly sensitive information and systems.

Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities, United States Department of Energy, August 19, 2002 (draft Version 1): General guidance on critical functions and assets, threats and vulnerabilities, and security enhancement.

Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments, United States Department of Energy, December 4, 2001 (draft Version 1.0): Tool for reviewing, updating, or conducting vulnerability and risk assessments.

FM 3-19.30, *Physical Security*, United States Department of the Army, 8 January 2001: Comprehensive manual on concepts and applications of physical security.

General Security Risk Assessment Guidelines, ASIS International, November 13, 2002: Methodology for security professionals by which security risks at a specific location can be identified and communicated, along with appropriate solutions.

MIL-HDBK-1013/1A, *Design Guidelines for Physical Security of Facilities*, Department of Defense, 15 December 1993: Manual providing guidance to ensure that appropriate physical security considerations are included in the design of facilities.

NFPA 730, *Guide for Premises Security*, National Fire Protection Association, September 19, 2003 (proposed draft): Descriptions of construction, protection, and occupancy features and practices intended to reduce security vulnerabilities to life and of property.

Security Guidelines for the Electricity Sector, North American Electric Reliability Council, June 14, 2002 (Version 1.0): Descriptions of general approaches, considerations, practices, and planning philosophies to be applied in protecting electric infrastructure systems.

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*, 31 July 2002: Appropriate, implementable, and enforceable measures to minimize the possibility of mass casualties in buildings or portions of buildings in the event of a terrorist attack.

Urgent Action Standard 1200, *Cyber Security*, North American Electric Reliability Council, August 13, 2003: Measures to reduce risks to the reliability of bulk electric systems from any compromise of critical cyber assets.

Vulnerability Assessment and Survey Program: Lessons Learned and Best Practices, United States Department of Energy, September 28, 2001: Summary of initial lessons learned and best practices captured by Office of Energy Assurance.

Vulnerability Assessment and Survey Program: Overview of Assessment Methodology, United States Department of Energy, September 28, 2001: High-level overview of vulnerability assessment methodology being developed and validated by Office of Energy Assurance.

Vulnerability Assessment Methodology: Electric Power Infrastructure, United States Department of Energy, September 30, 2002 (draft): Detailed description of a methodology that has been applied to the electric power infrastructure.

WECC Guidelines for Minimum Physical Security of Control Centers, Western Electricity Coordinating Council, March 4, 2003 (draft): Guidelines on the physical security of control centers including communications equipment (e.g. SCADA) located therein.