Supplementary Material

Appendix Table. Examples of Risks for Responsible Officials to Consider

Physical security	• Physical access controlled by computerized system could be insecurely configured—eg, not changing the default password on a physical security system. • Biometric failures, in which an attacker uses fake fingerprints. • Records of master keys could be kept in a computer application and let an attacker know who has key access. • If the intrusion detection system is connected to a network, it could be disabled over the network. • If an emergency person-down system uses wireless for communications, it could be disrupted by wireless outage or jammed.
Access control	• An IT helpdesk employee could be bribed into resetting password of an administrator or someone who has access to the select agent data or systems. • The transient nature of students and many higher education organizations can make access control difficult. If a student, researcher, or staff person is working in a registered space, but also is engaged with other parts of the university, access may linger unless it is specifically removed when someone no longer needs to access the data or space, but could still retain an account or physical access. • The confidentiality could be breached accidentally, sharing what is in inventory.
Medical and research devices	• Centrifuge, pump, or other medical or research device connected to a computer connected to a network could be compromised over the network, allowing an attacker to gain control of the device.
Inventory[1]	• An attacker could modify inventory: add, remove, or change contents electronically without entering physical space. • Inventory data could be deleted or lost accidentally if not properly backed up.
Monitoring the environment	• If email is used for communications around the security of the environment or movement of inventory, the email could be compromised. • Audio or video communications over an IP network (intra-room communication) could be compromised to monitor movement in the lab or potentially contents of the inventory. • A system used for remote observation or monitoring
Environmental	• If the HVAC system is controlled by a computer connected to a network, it could have its setting maliciously configured to change the air pressure. • If lights or electricity are controlled by a computer connected to a network, the light or electricity could be turned off. • If the computer network is compromised or disabled, all of the systems that rely on it could potentially be compromised or disabled.

[1] *Guidance on the Inventory of Select Agents and Toxins.* US Centers for Disease Control and Prevention; Animal and Plant Health Inspection Service (APHIS). June 20, 2014. http://www.selectagents.gov/resources/Long_Term_Storage_version_3.pdf. Accessed April 15, 2015.