



June 22, 2018

MEMORANDUM FOR: REGIONAL COMMISSIONERS, PBS
REGIONAL LEASING DIRECTORS
REGIONAL LEASE ACQUISITION OFFICERS

FROM: ALLISON AZEVEDO 
ASSISTANT COMMISSIONER FOR OFFICE OF LEASING -
PR

SUBJECT: LEASING ALERT (LA-FY18-05) Cybersecurity Measures for
Leased Facilities

1. Purpose. This Leasing Alert provides required and recommended measures for lessors related to cybersecurity protections and precautions in leased facilities. It establishes lease language that prohibits lessors from connecting any portion of their building and access control systems (BACS) to any federally-owned or operated IT network and requires notification for cybersecurity incidents that impact a federal tenant's safety, security, or proper functioning. The lease language also outlines recommended cybersecurity measures that lessors are encouraged to follow.

2. Background. Cybersecurity protections in leased space focus on safeguarding BACS, which provide fire and life safety control, physical access control, building power and energy control, electronic surveillance, and automated HVAC, elevator, and building systems monitoring and control. The increased connectivity of BACS to other information systems and the external internet make them vulnerable to unauthorized access, system abuses, and uncontrolled disruptions. A range of cyber threats to BACS could compromise security measures that impact an agency's ability to carry out their mission, or cause damage to facilities and harm to occupants.

Cybersecurity measures were developed in response to GAO Report 15-6 from December 2014, entitled "DHS and GSA Should Address Cyber Risk to Building and Access Control Systems". This GAO report explored the ability of agencies to address cyber threats to BACS in federal facilities, and the ability of agencies to protect federal facilities from cyber attacks and vulnerabilities. GAO recommended for: a) DHS to develop a strategy to address cyber risks to BACS; b) GSA to more fully assess cyber risks of BACS using Federal Information Security Management Act of 2002 (FISMA) guidelines; and c) the Interagency Security Council (ISC) to revise guidance to include countermeasures for cyber threats to BACS.

The Office of Leasing collaborated with GSA's Office of the Chief Information Officer (OCIO), Office of Mission Assurance (OMA), Office of Governmentwide Policy (OGP), and the PBS Office of Facilities Management (OFM) to develop a set of required and recommended measures for lessors to protect against cybersecurity threats.

- a) **Required measures** include prohibiting Lessors from connecting any portion of their BACS to any federally-owned or operated IT network and requiring Lessors to notify the Government in the event of a cybersecurity incident.
- b) **Recommended guidance** includes cybersecurity and IT industry best practices that Lessors are encouraged to follow in order to protect their BACS systems, including, standards related to system configuration, encryption, proper access, antivirus software, password protection, software patching, proper disabling, etc.

3. Effective Date. This Leasing Alert is effective as of the date of issuance unless modified, canceled, or reissued.

4. Cancellation. Facility Security Level (FSL) Templates I through IV, originally issued via Lease Acquisition Circular (LAC) 2012-06. Note that additional changes to these FSL templates, incorporating updated Interagency Security Committee (ISC) countermeasures, will be issued via a future Leasing Alert to be issued later this Fiscal Year.

5. Applicability. This Leasing Alert and its attachments apply to all General Services Administration (GSA) real property leasing and to activities delegated by GSA to other Federal agencies.

6. Instructions and Procedures.

Attachment 1 includes new cybersecurity requirements which have been added to all four (4) Facility Security Level (FSL) templates (FSL I through FSL IV). LCOs must use the appropriate revised FSL template containing the updated cybersecurity language for RLPs issued on or after the effective date of this Leasing Alert. For projects where negotiations have not closed, LCOs must issue an amendment that includes the revised FSL template.

As indicated above, the cybersecurity language includes both required and recommended practices, including a notification protocol for the Lessor to follow when there is a cyber incident within a leased facility.

Note that, in the event of a **cybersecurity incident** within a leased facility, there are roles and responsibilities for different affected parties, as outlined below:

- i) The Lessor initially assesses the cyber incident (related to their BACS), and identifies the impacts and risks to the building and its occupants. Lessors should

- follow their organization's procedures and protocols related to containing and handling a cybersecurity incident.
- ii) The Lessor immediately informs the Lease Contracting Officer's (LCO's) designated representative, i.e., the Lease Administration Manager (LAM), about cyber incidents that impact a federal tenant's safety, security, or proper functioning (based on the Lessor's assessment).
 - iii) The LAM informs the tenant agency about BACS-related cyber incidents that could impact their safety, security, or proper functioning. For cybersecurity and IT issues within a tenant agency's internal systems, tenants should follow guidance provided by their specific agency.
 - iv) The LAM informs the Lease Contracting Officer (LCO) about significant cybersecurity incidents that impact a tenant's safety and functioning and will take necessary lease enforcement steps.

ATTACHMENT 1: Cybersecurity for Leased Facilities (added to all FSL templates)

Attachment 1

Cybersecurity for Leased Facilities

(Language added to all FSL templates June 2018)

- A. Lessors are **prohibited** from connecting any portion of their building and access control systems (BACS) to any federally-owned or operated IT network. BACS include systems providing fire and life safety control, physical access control, building power and energy control, electronic surveillance, and automated HVAC, elevator, or building monitoring and control services (including IP addressable devices, application servers, or network switches).

- B. In the event of a **cybersecurity incident** related to BACS, the Lessor shall initially assess the cyber incident, identify the impacts and risks to the Building and its occupants, and follow their organization's cyber and IT procedures and protocols related to containing and handling a cybersecurity incident. In addition, the Lessor shall immediately inform the Lease Contracting Officer's (LCO's) designated representative, i.e., the Lease Administration Manager (LAM), about cybersecurity incidents that impact a federal tenant's safety, security, or proper functioning.

- C. Lessors are **encouraged** to put into place the following cyber protection measures in order to safeguard facilities and occupants:
 1. Engineer and install BACS to comply with the Department of Homeland Security Industrial Control Systems Computer Emergency Response Team (DHS ICS-CERT) cyber security guidance and recommendations (<https://ics-cert.us-cert.gov/Recommended-Practices>).
 2. Refer to the National Institute of Standards and Technology Cyber Security Framework (NIST-CSF) (<https://www.nist.gov/cyberframework>) and cybersecurity guidance in the DHS Commercial Facilities Sector-Specific Plan (<https://www.dhs.gov/publication/nipp-ssp-commercial-facilities-2015>) for best practices to manage cyber risks.
 3. Encourage vendors of BACS to secure these devices and software through the following:
 - a. Develop and Institute a proper Configuration Management Plan for the BACS devices and applications, so that the system can be supported.
 - b. Safeguard sensitive data and/or login credentials through the use of strong encryption on devices and applications. This means using NIST- approved encryption algorithms, secure protocols (i.e., Transport Layer Security (TLS) 1.1, TLS 1.2, TLS 1.3) and Federal Information Processing Standard (FIPS) 140-2 validated modules.
 - c. Disable unnecessary services in order to protect the system from unnecessary access and a potential exposure point by a malicious attacker. Examples include File Transfer Protocol-FTP (a protocol used for transferring files to a remote location) and Telnet (allowing a user to issue commands remotely). Additionally use of protocols that transmit data in the

clear (such as default ZigBee) should be avoided, in favor of protocols that are encrypted.

- d. Close unnecessary open ports to secure against unprivileged access.
- e. Monitor and free web applications and supporting servers of common vulnerabilities in web applications, such as those identified by the (Open Web Application Security Project (OWASP) Top 10 Project (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)).
- f. Enforce Least Privilege, where proper permissions are enforced on a device or application so that a malicious attacker cannot gain access to all data. Enforcing Least Privilege will only allow users to access data they are allowed to see. Additional information can be found at <https://www.beyondtrust.com/blog/what-is-least-privilege/>
- g. Protect against Insufficient User Access Auditing, where device or application does not have a mechanism to log/track activity by user. Enforce changing of factory default Username and Password to prevent unauthorized entry into the BACS system.
- h. Use updated antivirus software subscription at all times. Kaspersky-branded products or services, prohibited from use by the Federal Government, are not to be utilized.
- i. Conduct antivirus and spyware scans on a regular basis. Patching for workstations and server Operating System (OS), as well as vulnerability patching should follow standard industry best practices for software development life cycle (SDLC).
- j. Discontinue the use of end of life (EOL) systems and use only applications/systems that are supported by the manufacturer.
- k. Operating Systems must be supported by the vendor for security updates (e.g., do not use Windows Server 2003).
- l. Proposed standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved United States Government Configuration Baseline (USGCB) or tenant agency guidance (if applicable).
- m. Disallow the use of commercially-provided circuits to manage building systems and install building systems on a protected network, safeguarded by the enterprise firewalls in place. Workstations or servers running building monitor and control systems are not connected and visible on the public internet.
- n. Systems should have proper system configuration hardening and align with Center for Internet Security ([CIS](https://www.cisecurity.org/cis-benchmarks/)) benchmarks or other industry recognized benchmarks. Additional information can be found at <https://www.cisecurity.org/cis-benchmarks/>.