GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

PBS 3490.3 CHGE 1
March 22, 2021

GSA ORDER

SUBJECT: Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property

1. Purpose. This Order describes the Public Buildings Service (PBS) policy to protect information related to Federal buildings, grounds, and property under the jurisdiction, custody, or control of the U.S. General Services Administration (GSA), including those properties delegated to other Federal agencies by the Administrator of General Services. For the purposes of this Order, all such buildings, grounds, and property are collectively referred to as "GSA-controlled space." Within the Controlled Unclassified Information (CUI) Program, this information is categorized as Physical Security information. Physical Security information is a category of CUI. This policy authorizes safeguarding and dissemination controls, established by the CUI Program, to be applied to Physical Security information. Not all building information for these buildings is automatically considered CUI. Only specific applicable information that qualifies and is marked as CUI needs to be controlled and protected in accordance with 32 C.F.R. part 2002. GSA will use CUI terminology and markings on all applicable building information in all formats, as described in greater detail in Appendix B. Building information marked as Sensitive But Unclassified (SBU) in accordance with previous versions of this policy (PBS 3490.2 series) must be protected and handled as CUI in accordance with 32 C.F.R. part 2002. Information that was marked as SBU does not need to be re-marked with CUI markings while it remains in the possession of an authorized holder within GSA; however, upon transfer or reuse (in derivative form) outside of GSA, the information must be marked or identified as CUI in accordance with 32 C.F.R. part 2002. All holders of this information must align protective measures to the standards of this Order and the CUI Program in 32 C.F.R. part 2002. Building occupancy data does not meet the definition of sensitive building information and is not covered by this Order.

2. Background.

a. GSA has been marking and managing SBU building information and has issued several updates to the policy relating to such information since the bombing of the Alfred Murrah Federal Building in 1995.

b. Executive Order 13556, signed on November 4, 2010, established a program for managing CUI, with the National Archives and Records Administration (NARA) serving as the executive agent. This executive order emphasizes the importance of "the openness and uniformity of Government-wide practice." GSA has been working with NARA to

develop CUI standards and best practices. NARA published its CUI implementing regulation at 32 C.F.R. part 2002 on September 14, 2016. Accordingly, GSA is replacing the GSA SBU designation with the executive branch-wide CUI designation and this Order implements the new CUI requirements for PBS building information in accordance with GSA Order CIO 2103.1, Controlled Unclassified Information (CUI) Policy, issued May 16, 2017.

3. Cancellation. This Order cancels and supersedes GSA Order PBS P 3490.2, Document Security for Sensitive but Unclassified Building Information, issued September 2, 2014.

4. Scope and Applicability. This Order applies to all entities that handle, receive, and store CUI building information related to GSA-controlled space, as well as to the access to and generation, dissemination, storage, transfer, and disposal of all such information. It also applies to procurements to acquire, alter, or manage space, either Government-owned or leased, including GSA space that is delegated to other Federal agencies. THIS ORDER DOES **NOT** APPLY TO BUILDING INFORMATION CLASSIFIED UNDER EXECUTIVE ORDER 13526, Classified National Security Information.

a. All sensitive building information must be marked and managed as CUI in accordance with 32 C.F.R. part 2002. Physical Security information is a category of CUI and must be marked in accordance with the CUI Program. The GSA Office of Information Technology Category (IT), along with PBS business lines, will develop a system to track project CUI building information. This system will be implemented in a phased approach and completed within five years of the issuance date of this Order.

b. Existing SBU building documents, marked prior to this revised Order, must be controlled and protected when procuring and contracting for design and construction services for renovations to existing facilities.

c. For new facilities, whether owned or leased, the building drawings and other related building information will be reviewed and must be designated CUI, as appropriate, in accordance with the “Specific Requirements and Responsibilities” section of this Order. The designation as CUI occurs when the information is turned over by the architect-engineering (A-E) personnel to the Government as part of the final approved concept-documents. Not all building information should be designated as CUI.

d. For GSA-leased building information, PBS has determined that procedures contained in this Order for access to and generation, dissemination, storage, transfer, and disposal of CUI building information apply to leased space for the following facility types:

(1) ISC Facility Security Level V GSA-leased facilities,

(2) ISC Facility Security Level IV GSA-leased facilities,

(3) ISC Facility Security Level III GSA-leased facilities with 100 percent Federal Government occupancy, or

(4) Other GSA-leased facilities to be considered when requested in writing by the certifying official of the customer agency, in accordance with the guidance in this Order.

5. Policy Objectives. This Order has two principal objectives:

a. To diminish the potential that CUI building information will be available for use by a person or persons with an interest in causing harm; and

b. To allow access to CUI building information only to those recipients who have a legitimate business need to know and a Lawful Government Purpose to access such information.

6. Definitions.

a. CUI Building Information (within the CUI Physical Security Category). Information related to GSA-controlled space that is sufficiently sensitive to warrant some level of protection from full and open public disclosure, but does not warrant classification. This information requires safeguarding and dissemination controls to diminish the potential that it will be accessible to a person or persons with an interest in causing harm. Appendix A provides a list of examples of CUI building information. This list is not exhaustive and is only intended to illustrate some of the more common examples of CUI Building Information.

b. Lawful Government Purpose. A Lawful Government Purpose is any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement). 32 C.F.R. § 2002.4(bb). An individual must have a Lawful Government Purpose to access CUI Building Information. Some examples of individuals who may have a Lawful Government Purpose are GSA project and facilities managers, staff from the Office of the Inspector General (OIG), authorized vendors, utilities, and state and local fire department personnel. This Order does not describe all instances of a legitimate Lawful Government Purpose.

7. Clarification for GSA Order CIO P 2181.1. All building drawings or building information should **not** be designated, automatically, as CUI. Refer to Appendix A of this document for guidance. GSA Order CIO P 2181.1 provides the policy and procedures for issuing and maintaining GSA credentials. Chapter 2, Section 4.b.(4) of GSA Order CIO P 2181.1 states, “Those individuals whose duties require a higher degree of trust, such as IT system administrators, those who handle financial transactions, or those who deal with PII, and other sensitive information (e.g., building drawings, etc.), will continue to require investigations associated with higher levels of trust such as the Minimum Background

Investigation (MBI) or the Limited Background Investigation (LBI).” GSA may grant access to individuals without GSA credentials when those individuals possess a Lawful Government Purpose to access such information.

8. Explanation of Changes.

a. Transmittal Page, Section 1, “authorized holder” changed to “authorized holder within GSA” and some language added;

b. Specific Requirements and Responsibilities, page 10, Section 14.a., some language removed;

c. Specific Requirements and Responsibilities, page 11, Section 14.b., some language removed;

d. Appendix C, Section 2.b. i., some language added.

9. Signature.

/S/
ALLISON H. AZEVEDO
Acting Commissioner
Public Buildings Service

Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property

Table of Contents

GENERAL REQUIREMENTS AND RESPONSIBILITIES

The principles governing the management of CUI building information are as follows:

1. CUI building information must be controlled so that building information in electronic and hardcopy formats is made available only to individuals who have a Lawful Government Purpose.

2. Adequate controls must be used to monitor access to and dissemination of CUI building information.

3. CUI building information must be safeguarded inside a controlled environment during use and either properly destroyed or returned to GSA after use. See 32 C.F.R. § 2002.14 for guidance regarding the safeguarding and destruction requirements for CUI.

4. CUI building information must not be presented in public forums unless required by jurisdictions having authority.

5. Whether a given building's information (for design, construction, facility management, or other PBS activities) is sensitive and qualifies as CUI, shall be based on whether the specific information needs safeguarding or dissemination controls, taking into account the security level of the building and any instructions included in a written request from a certifying official of an occupant agency.

6. For leased space, the procedures outlined in this Order for access to and generation, dissemination, storage, transfer, and disposal of CUI building information apply to the following facility types:

(1) ISC Facility Security Level V GSA-leased facilities,

(2) ISC Facility Security Level IV GSA-leased facilities,

(3) ISC Facility Security Level III GSA-leased facilities with 100 percent Federal Government occupancy, or

(4) Other GSA-leased facilities to be considered when requested in writing by the certifying official of the occupant agency, in accordance with the guidance in this Order.

7. GSA employees must have, at a minimum, a Moderate Risk, Public Trust or higher security clearance to designate physical security information as CUI.

SPECIFIC REQUIREMENTS AND RESPONSIBILITIES

1. Public Buildings Service. PBS is ultimately responsible for protecting CUI building information from unauthorized use and for making the initial determination of whether information relating to an entire building, or portion thereof, is considered CUI.

2. PBS Regional Commissioners. Each PBS Regional Commissioner (RC) or their authorized designee (or in the case of delegated buildings, an authorized agency official), makes the initial determination regarding whether a building's documents/information or a portion thereof qualify as CUI. That determination will, in turn, trigger action on the part of the PBS Project Manager or Program Manager to mark the necessary related building information as CUI.

a. The RC must consider the security level of the building itself, as well as comparable building types and the occupant agencies when making the determination whether or not a building's documents/information, or a portion thereof, qualify as CUI.

b. The RC must designate an individual in their respective region responsible for controlling CUI building information.

c. The RC must implement this Order within their region in a uniform, consistent manner so that all items containing CUI building information are marked and handled appropriately.

d. In the case of a new building in the planning stages for a single occupant agency, the RC, in consultation with the occupant agency, has decision-making authority to determine whether the building information qualifies as CUI.

e. In the case of a new building in the planning stages for multiple occupant agencies, the RC, in consultation with all projected occupant agencies, has the decision-making authority in determining whether the building information qualifies as CUI.

f. For GSA-leased space, PBS has determined that procedures contained in this Order for access to and generation, dissemination, storage, transfer, and disposal of CUI building information apply to leased space for the following facility types:

(1) ISC Facility Security Level V GSA-leased facilities,

(2) ISC Facility Security Level IV GSA-leased facilities,

(3) ISC Facility Security Level III GSA-leased facilities with 100 percent Federal Government occupancy, or

(4) Other GSA-leased facilities to be considered when requested in writing by

the certifying official of the occupant agency, in accordance with the guidance in this Order.

3. Customer Agencies. In cases where a customer agency requests building information to be categorized as a controlled document (when not otherwise required by CUI policy), GSA requires the customer agency to pay any extra costs associated with higher security requirements. The customer agency must agree to fund such costs through either a reimbursable work authorization or rent, as applicable. Extra costs may be due to limits on the A-E, personnel access, bidding restrictions, reduced competition for construction and facility management, or other factors related to the customer agency's security. The RC or their designee will assist the customer agency in identifying the additional costs associated with its request and requirements.

a. The determination of whether the building's information qualifies as CUI is not affected by the customer agency's request that building information be categorized as a controlled document except as provided in paragraphs 5 and 6 of the General Requirements and Responsibilities, above. If the building information requires safeguarding or dissemination controls, it qualifies as CUI within the Physical Security category; if it does not, then it is Uncontrolled Unclassified Information.

b. Within a Federal campus, the CUI designation may apply to information relating to one or more buildings in the campus, as needed, but will not automatically apply to all buildings' information within the same campus.

4. PBS Project, Program, or Facility Manager. The PBS Project or Program Manager (PM) or the PBS Facility Manager (FM), as applicable, is responsible for reviewing all building documents, identifying and marking CUI, and including instructions in Statements of Work for contractors to mark documents as CUI, if appropriate.

5. Mandatory Review. For building projects (for design, construction, facility management, and other PBS activities), the PBS PM or FM, as applicable, is responsible for reviewing all building information that contains or may contain CUI at regular milestones (such as change in use, configuration or occupant agency); and for identifying and validating that CUI markings are correct. If the CUI designation is found to be incorrectly marked or no longer required, the PBS PM or FM, as applicable, must promptly take corrective action to change or remove the marking.

6. Facility Security Committee. Except for GSA-leased space, either during design development or after construction is complete, the building's Facility Security Committee (FSC) or its current equivalent, as outlined in the Risk Management Process established by the ISC, must advise the PBS PM or FM, as applicable, regarding additional specific building information where CUI markings are necessary.

a. The FSC, or its current equivalent, may determine that some specific building information for that building qualifies as CUI. In this case, the FSC must advise the PM or FM, as applicable, to mark only that specific building information as CUI. The FSC

must refer to Appendix A of this Order for further guidance.

b. The FSC, or its current equivalent, may determine that some specific building information no longer qualifies as CUI. In this case, the FSC must advise the PM or FM, as applicable, to mark only that specific building information that is CUI. The FSC must refer to Appendix A of this Order for further guidance.

6. Disseminators. Disseminators of CUI building information must comply with the policy, principles and requirements of this Order. CUI building drawings that are part of a procurement must be issued in accordance with Federal Acquisition Regulation (FAR) § 5.102(a)(4) on the secure side of the SAM.gov website (https://sam.gov/SAM/), or any successor system, with proper document control protocols to allow legitimate registered vendors access to the documents for proposing and pricing the procurements.

7. Contracting Officers. The Contracting Officer (CO) must include the clause in Appendix C, or a similar updated clause per the GSA Acquisition Manual (GSAM), in all solicitations (including Requests for Lease Proposals (RLPs)), building contracts, and leases that may contain, require access to, or cause the generation of CUI building information. This applies to all contracts issued after issuance of this Order.

a. Examples of such contracts are A-E design, construction and facility management, and related professional service contracts, such as Construction Manager as Advisor and Commissioning Authority contracts.

b. COs must take appropriate action when they become aware that contractors have not fulfilled contractual obligations regarding the protection of CUI building information. Such action may include an investigation, referring the contractor for suspension or debarment proceedings, terminating the contract for default, or any combination of the foregoing.

8. GSA Employees (And Other Authorized Holders). GSA employees and other authorized holders may disseminate CUI building information only after determining whether the recipient has a Lawful Government Purpose.

9. General Counsel. The Office of General Counsel (OGC) provides legal advice concerning Freedom of Information Act (FOIA) requests that apply to CUI building information. OGC also provides counsel regarding the application of this Order.

10. PBS Regional Commissioners, Assistant Commissioners and Deputy Assistant Commissioners. The PBS RCs, Assistant Commissioners, and Deputy Assistant Commissioners must make their respective personnel aware of the requirements in this Order, and require that their staffs be trained in the proper application of this Order, including encryption software applications available to GSA personnel and contractors.

11. Marking Information. For any CUI building information created after the issuance date of this Order, pages containing CUI building information must follow NARA's Marking Controlled Unclassified Information (CUI) Handbook identified in Appendix B.

12. Limiting Dissemination to Authorized Recipients. CUI building information may be disseminated only after it is determined by GSA personnel that each recipient is authorized to receive it. The criterion to determine whether a recipient is authorized to receive CUI building information is that the recipient must have a Lawful Government Purpose for access, as described in section 4 (Scope and Applicability) of the transmittal for this Order.

a. Federal, State, and Local Government Entities. GSA must provide CUI building information for the performance of official Federal, state, and local government functions, such as inspections, OIG audits, code compliance reviews, and issuance of building permits, among other purposes. Public safety entities, such as fire departments, may be determined to have a Lawful Government Purpose to access CUI building information on a case-by-case basis. This Order must not prevent or encumber the necessary dissemination of CUI building information to such public safety entities.

b. Vendors, Non-Governmental Entities and Utilities. Unless the action is exempt under FAR § 4.1102, all disseminators are responsible for verifying that a vendor is currently registered as "active" in the System of Award Management (SAM) database at www.sam.gov, or any successor system, and also has a Lawful Government Purpose before providing the information to the vendor. Non-governmental entities and utility companies may also have a Lawful Government Purpose requiring access to CUI building information for the performance of work on GSA-controlled space on a case-by-case basis, and do not necessarily need to register within the SAM database.

13. Electronic Transmission of CUI Building Information. GSA employees and other authorized holders who electronically transmit CUI building information outside of the GSA network must encrypt the data with an approved National Institute of Standards and Technology (NIST) algorithm, such as Advanced Encryption Standard (AES), in accordance with Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules.

14. Dissemination of CUI Building Information in Non-Electronic Form or on Portable Electronic Data Storage Devices. Portable electronic data storage devices include CDs, DVDs, and USB drives. Files on these devices must be encrypted with an approved NIST algorithm. Non-electronic forms of CUI building information include paper documents.

a. By Mail. GSA employees must only use methods of shipping that provide confirmation of receipt of the CUI building information, such as track and confirm, proof of delivery, signature confirmation, or return receipts. CUI markings must not appear on the exterior of packages.

b. In person. GSA employees may only provide CUI building information to authorized representatives of Federal, state, and local government entities, SAM-registered firms, and others that have a Lawful Government Purpose to access such information.

15. Safeguarding CUI Building Information. GSA employees and other authorized holders must not take CUI building information outside of GSA facilities, except as necessary for the performance of a GSA project. If a GSA employee or other authorized holder takes CUI building information outside of a GSA facility, access to the information must be limited to only those with a Lawful Government Purpose for access. Such information must be returned to a GSA facility or destroyed when no longer needed for the performance of a GSA project. CUI building information must be stored in a controlled environment that prevents unauthorized access (*e.g.,* locked rooms or cabinets).

16. Media Storage. GSA employees and embedded contractors must not store or retain CUI building information on any electronic device or media not issued or approved by GSA.

17. Destroying CUI Building Information. When CUI building information, in any format, is no longer needed, it must be destroyed in accordance with NIST Special Publication 800-88, Guidelines for Media Sanitization. Alternatively, the CUI building information may be returned to the CO.

18. FOIA Requests. CUI markings do not control the decision of whether to disclose or release the information to any entity that files a FOIA request. Any determination to disclose CUI building information in response to a FOIA request must be made after consultation with OGC.

19. Reporting CUI Security Incidents. Any actual or suspected unauthorized disclosure of CUI must be reported immediately to the CO for the related contract or the appropriate RC. RCs are required immediately to notify the FSC for the building involved. Any incident involving suspected computer or cyber security breach or attack, as defined by NIST Special Publication 800-61, Computer Security Incident Handling Guide, must be reported in accordance with the current version of CIO 2100.1 GSA Information Technology Security Policy, and the GSA CIO IT Security Procedural Guide: CIO-IT Security-01-02, Incident Response (IR).

- Authorized holders and all GSA employees are responsible for reporting incidents of misuse involving CUI. Specific actions include:

  - **Employees and embedded contractors**: Notify the IT Service Desk at 866-450-5250 or ITServiceDesk@gsa.gov immediately.

- **Contractors:** Contractors are responsible for reporting incidents in accordance with the requirements of their contract(s). Two FAR cases have been opened to incorporate the applicable incident reporting requirements for Personally Identifiable Information and CUI into the FAR.

- **Leases:** For leases involving CUI (previously SBU), the lessor is responsible for reporting incidents to the Lease Contracting Officer and the GSA Incident Response Team at gsa-ir@gsa.gov.

Appendix A. Examples of CUI Building Information

Not all building information is automatically considered CUI. After the PBS PM or FM, as applicable, has reviewed, identified, and marked CUI building information, access to the information must be controlled. CUI building information may be contained in any document (including drawings, specifications, virtual modeling, reports, studies, or analyses) and in any format with information pertaining to:

1. Location and details of secure functions or secure space in a building, location or space. Examples include:

    a. Prisoner, detainee or judges' secure circulation paths or routes (both vertical and horizontal)
    b. Detention or holding cells
    c. Sally ports
    d. Security areas, including control rooms, Sensitive Compartmented Information Facilities, and incident command centers
    e. Building automation systems (BAS)
    f. Communication centers, telephone and riser closets
    g. Utilities, fuel and power distribution

2. Location and type of structural framing for the building, including any information regarding structural analysis. Examples include information related to:

    a. Progressive collapse
    b. Seismic
    c. Building security
        i. Blast mitigation
        ii. Counterterrorism methods taken to protect the occupants and the building

3. Risk assessments and information regarding security systems or strategies of any kind. Examples include:

    a. Camera locations
    b. Nonpublic security guard post information (*e.g.*, number, location, or operations)
    c. Electronic control systems
    d. Hardware and key control

Note: In the case of building information related to a specific suite, room/space, or other component's information that is designated as CUI (*e.g.*, BAS diagrams or security camera layout), the CUI designation does not necessarily carry over to the entire building's information, nor to the entire campus.

Note: Building information for a stand-alone steam plant facility or similar service facility and its associated tunnels must be designated CUI when it services a building that is designated as sensitive.

Note: Drawings marked as CUI may not require that associated specifications be marked CUI if they are general in nature, and do not relate to the definition of CUI building information.

Shop drawings also need to be marked as CUI when they relate to design drawings marked as CUI.

GSA Office of Facilities Management (OFM) is responsible for controlling historic documents not previously marked as SBU that would qualify as CUI, and must manage them accordingly.

Legacy information is unclassified information that was marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program. Legacy information is not automatically CUI. Individual facility management teams must examine and determine what legacy information qualifies as CUI and mark it accordingly.

Building occupancy data does not meet the definition of sensitive building information and is not covered by this Order.

In cases of excessive burden, GSA's Senior Agency Official for CUI may issue a "Legacy Marking Waiver," as described in 32 C.F.R. § 2002.38(b) of the CUI Rule. When such a waiver is granted, legacy material that qualifies need not be re-marked as CUI until and unless it is to be "re-used" in a new document or dissemination.

Appendix B. CUI Marking

1. In any **electronic or printed document**, pages containing CUI building information must comply with the current version of NARA's Marking CUI Handbook found on its CUI website.

2. The CUI markings must be used regardless of the medium through which the information appears or is conveyed.

3. **CUI Marking Guide Specific to Construction Drawings and Specifications**

CUI Banner Marking – All CUI building information construction documents must follow the banner marking guidelines established in "Part One: CUI Markings in an Unclassified Environment" of NARA's Handbook.

Designation Indicator – All documents containing CUI building information must indicate that GSA is the designating agency and identify primary point of contact name, phone number and email.

If the document contains both CUI and uncontrolled unclassified information, the document may be portion marked. If portion marking is used, the CUI portions must be marked "CUI" and non-CUI portions must be marked with a "U" to indicate that that portion is uncontrolled unclassified Information. The index sheet will identify drawings, sections, and specifications that contain CUI.

Separate parts of the document (such as appendices or attachments) that do not contain information that requires controlling will not be marked with a CUI banner or CUI portion marking.

Appendix C. CUI Contract Clause

COs must include the following clause, or a similar updated clause per the GSAM, in: (1) all solicitations containing CUI building information (including Requests for Lease Proposals or Solicitations for Offers); and (2) contracts and final leases that may contain, require access to, or cause the generation of CUI building information.

Contractors must continue to handle sensitive building information as required under already existing contracts until the contract is modified to include the clause below or another CUI contract requirement applies.

[Begin clause]

Safeguarding and Dissemination of Controlled Unclassified Information (CUI) Building Information

This clause applies to all recipients of CUI building information (which falls within the CUI Physical Security category), including offerors, bidders, awardees, contractors, subcontractors, lessors, suppliers and manufacturers.

Marking CUI. Contractors must submit any contractor-generated documents that contain building information to GSA for review and identification of any CUI building information that may be included. In addition, any documents GSA identifies as containing CUI building information must be marked in accordance with the Order and the Marking Controlled Unclassified Information Handbook (the current version may be found at https://www.archives.gov/files/cui/20161206-cui-marking-handbook-v1-1.pdf) before the original or any copies are disseminated to any other parties. If CUI content is identified, the CO may direct the contractor, as specified elsewhere in this contract, to imprint or affix CUI document markings (CUI) to the original documents and all copies, before any dissemination, or authorized GSA employees may mark the documents.

1. Authorized recipients.

   a. Building information designated as CUI must be protected with access strictly controlled and limited to those individuals having a Lawful Government Purpose to access such information, as defined in 32 C.F.R. § 2002.4(bb). Those with such a Lawful Government Purpose may include Federal, state and local government entities, and non-governmental entities engaged in the conduct of business on behalf of or with GSA. Non-governmental entities may include architects, engineers, consultants, contractors, subcontractors, suppliers, utilities, and others submitting an offer or bid to GSA, or performing work under a GSA contract or subcontract. Recipient contractors must be registered as “active” in the System for Award Management (SAM) database at www.sam.gov, and have a Lawful Government Purpose to access such information. If a subcontractor is not registered in the SAM database and has

a Lawful Government Purpose to possess CUI building information in furtherance of the contract, the subcontractor must provide to the contractor its DUNS number or its tax ID number and a copy of its business license. The contractor must keep this information related to the subcontractor for the duration of the contract and subcontract.

b. All GSA personnel and contractors must be provided CUI building information when needed for the performance of official Federal, state, and local government functions, such as for code compliance reviews and the issuance of building permits. Public safety entities such as fire and utility departments may have a Lawful Government Purpose to access CUI building information on a case-by-case basis. This clause must not prevent or encumber the necessary dissemination of CUI building information to public safety entities.

2. Dissemination of CUI building information:

a. By electronic transmission. Electronic transmission of CUI information outside of the GSA network must use session encryption (or alternatively, file encryption) consistent with National Institute of Standards and Technology (NIST) SP 800-171. Encryption must be through an approved NIST algorithm with a valid certification, such as Advanced Encryption Standard or Triple Data Encryption Standard, in accordance with Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, as required by GSA policy.

b. By nonelectronic form or on portable electronic data storage devices. Portable electronic data storage devices include CDs, DVDs, and USB drives. Non-electronic forms of CUI building information include paper documents, photographs, and film, among other formats.

i. By mail. Contractors must only use methods of shipping that provide services for monitoring receipt such as track and confirm, proof of delivery, signature confirmation, or return receipt. CUI markings must not appear on the exterior of packages.

ii. In person. Contractors must provide CUI building information only to authorized recipients with a Lawful Government Purpose to access such information. Further information on authorized recipients is found in section 1 of this clause.

3. Record keeping. Contractors must maintain a list of all entities to which CUI is disseminated, in accordance with sections 2 and 3 of this clause. This list must include, at a minimum: (1) the name of the state, Federal, or local government entity, utility, or firm to which CUI has been disseminated; (2) the name of the individual at the entity or firm who is responsible for protecting the CUI building information, with access strictly controlled and limited to those individuals having a Lawful Government

Purpose to access such information; (3) contact information for the named individual; and (4) a description of the CUI building information provided. Once “as built” drawings are submitted, the contractor must collect all lists maintained in accordance with this clause, including those maintained by any subcontractors and suppliers, and submit them to the CO. For Federal buildings, final payment may be withheld until the lists are received.

4. Safeguarding CUI documents. CUI building information (both electronic and paper formats) must be stored within controlled environments that prevent unauthorized access. GSA contractors and subcontractors must not take CUI building information outside of GSA or their own facilities or network, except as necessary for the performance of that contract. Access to the information must be limited to those with a Lawful Government Purpose for access.

5. Destroying CUI building information. When no longer needed, CUI building information must either be returned to the CO or destroyed in accordance with guidelines in NIST Special Publication 800-88, Guidelines for Media Sanitization.

6. Notice of disposal. The contractor must notify the CO that all CUI building information has been returned or destroyed by the contractor and its subcontractors or suppliers in accordance with paragraphs 4 and 5 of this clause, with the exception of the contractor's record copy. This notice must be submitted to the CO at the completion of the contract to receive final payment. For leases, this notice must be submitted to the CO at the completion of the lease term.

7. CUI security incidents. All improper disclosures or receipt of CUI building information must be immediately reported to the CO and the GSA Incident Response Team Center at gsa-ir@gsa.gov. If the contract provides for progress payments, the CO may withhold approval of progress payments until the contractor provides a corrective action plan explaining how the contractor will prevent future improper disclosures of CUI building information. Progress payments may also be withheld for failure to comply with any provision in this clause until the contractor provides a corrective action plan explaining how the contractor will rectify any noncompliance and comply with the clause in the future.

8. Subcontracts. The contractor and subcontractors must insert the substance of this clause in all subcontracts.

[End of clause]