

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

PBS 3490.1A
June 1, 2009

GSA ORDER

SUBJECT: Document security for sensitive but unclassified building information

1. Purpose. This Order outlines the Public Buildings Service's (PBS's) policy on access to and generation, dissemination, storage, transfer, and disposal of sensitive but unclassified (SBU) building information concerning space controlled by the General Services Administration (GSA), including owned, leased, or delegated Federal facilities. Examples of SBU building information are listed in Attachment 1. An important goal of GSA is the safety and security of the people and facilities under GSA's charge and control. This Order promulgates the PBS security procedures needed to reduce the risk that SBU building information will be used for dangerous or illegal purposes. This Order is not intended to limit the sharing of SBU building information among GSA associates with a need to know such information to perform their assigned duties.
2. Cancellation. PBS 3490.1, Document Security for Sensitive But Unclassified Paper and Electronic Building Information, issued March 8, 2002, is cancelled. PBS 3490.1 canceled PBS-IL-01-03, Dissemination of Sensitive But Unclassified Paper and Electronic Design and Construction Documents, issued July 30, 2001.
3. Objectives. PBS's policy on SBU building information has two principal objectives to reduce exposure to possible attacks or threats to GSA-controlled space:
 - a. To diminish the potential that sensitive information about a building will be available for use by a person or persons with an interest in causing harm to persons or property.
 - b. To respect GSA's legitimate business needs to allow access to this information to those authorized recipients who have a need to know such information.
4. History. The protection of Federal employees, the public, and its facilities has always been a priority for GSA. Since the Alfred P. Murrah Federal Building bombing in Oklahoma City, Oklahoma on April 19, 1995, GSA has made a concerted effort to prevent another such occurrence. This revision of GSA Order 3490.1 provides updated guidance to reflect changes issued by, among others, the National Institute of Standards and Technology (NIST) on information technology (IT) security and Federal acquisition policies. This revision also takes into consideration the White House's May 9, 2008, memorandum entitled "Designation and Sharing of Controlled Unclassified Information" (CUI). This memorandum adopted "Controlled Unclassified Information" as the single designation throughout the executive branch for all information within the scope of that definition, including SBU, and directed the National Archives and Records Administration (NARA) to implement by May 2013 a single set of policies and procedures governing the designation, marking, safeguarding, and dissemination of such information. NARA suggested that GSA continue its use of the SBU designation until NARA implements the CUI policies and procedures.
5. Definitions.
 - a. Sensitive But Unclassified (SBU) building information is contained in any document with information that is sufficiently sensitive to warrant some level of protection from disclosure but that does not warrant classification.

- b. GSA-leased building information. GSA has determined that procedures for access to and generation, dissemination, storage, transfer and disposal of SBU building information pertain to leased space in a facility that has been designated:
- i. Interagency Security Committee (ISC) Facility Security Level IV GSA-leased facilities, or
 - ii. ISC Facility Security Level III GSA-leased facilities with 100 percent Government occupancy, or
 - iii. Other GSA-leased facilities will be considered, when requested in writing by the certifying official of the customer agency, in accordance with the guidance in this Order.

6. Application. This Order applies to the generation, dissemination, storage, transfer and disposal of all SBU building information about GSA-controlled space and to procurements to obtain, alter, or manage GSA-controlled space, either Government owned or leased, including GSA space that is delegated to other Federal agencies. This Order applies to all PBS associates.

This Order does not apply to information classified for national security purposes, which must be handled according to Department of Defense (DOD) 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), available at <http://www.dtic.mil/whs/directives/corres/html/522022m.htm>; GSA Acquisition Manual (GSAM) 504.4, Safeguarding Classified Information Within Industry; and other appropriate national security directives. Procurement sensitive information must be handled in accordance with the Procurement Integrity Act, 41 U.S.C. 423, as implemented under Federal Acquisition Regulation (FAR) 3.104.

7. Related authorities. This Order supports the use of the Federal Technical Data Solution (FedTeDS) discussed in FAR 5.102(a) (4), Availability of Solicitations.

8. Responsibilities.

- a. General. The principles governing the management of SBU building information are as follows:

- SBU building information must be disseminated only to authorized recipients who have a need to know such information.
- Adequate controls must be in place to monitor access to and dissemination of SBU building information.
- SBU building information must be safeguarded during use and destroyed properly after use.
- The more open the forum, the more generic or conceptual the information disseminated must be.

Disseminators of SBU building information are responsible for providing the first line of defense against misuse. This Order describes the effort generally required for adequate management of SBU building information. Disseminators of SBU building information must make every effort to comply with the principles above and all other requirements of this Order. In circumstances requiring adaptation of the other requirements of this Order, disseminators must apply the principles above and otherwise use good judgment, common sense and reasonableness.

- b. PBS Regional Commissioners (RCs), or their delegated PBS associates (or in the case of delegated buildings, agency officials), are ultimately responsible for protecting SBU building information from unauthorized use. RCs must implement this Order within their regions in a uniform, consistent manner so that documents containing SBU building information are marked and handled appropriately.

- c. PBS associates. PBS associates must disseminate SBU building information only after a proper review and the imprinting or affixing of a mark as required by this Order.

PBS associates are responsible for determining that the recipient of SBU building information is authorized to receive such information.

- d. General Counsel. The Office of General Counsel (OGC) can provide legal advice concerning Freedom of Information Act (FOIA) requests pertaining to SBU building information and can provide counsel regarding the application of this Order.
- e. The following officials must make their respective PBS associates aware of the requirements in this Order and require that their respective associates are trained in the proper application of this Order:
- Chief Architect, Office of the Chief Architect
 - PBS RCs
 - Assistant Commissioner for Design & Construction
 - Assistant Commissioner for the Office of Real Estate Acquisition
 - Assistant Commissioner for the Office of Facilities Management and Service Programs
 - Deputy Assistant Commissioner, Vendor Alliance and Vendor Acquisition
- f. PBS project team members are responsible for reviewing all documents containing building information (e.g., drawings, specifications, scopes of work), identifying and marking SBU building information, and including instructions in scopes of work (SOW) for contractors to mark documents as SBU, if applicable.

- (1) Marking information. Within any electronic or printed document, pages containing SBU building information must have the following mark imprinted or affixed:

**SENSITIVE BUT UNCLASSIFIED (SBU)
PROPERTY OF THE UNITED STATES GOVERNMENT
FOR OFFICIAL USE ONLY
Do not remove this notice
Properly destroy or return documents when no longer needed**

- (2) The following mark must be affixed to the cover or first page of any document (such as the cover page on a set of construction drawings) containing pages marked as required by paragraph (1) above:

**SENSITIVE BUT UNCLASSIFIED (SBU)
PROPERTY OF THE UNITED STATES GOVERNMENT
COPYING, DISSEMINATION, OR DISTRIBUTION OF THIS DOCUMENT TO UNAUTHORIZED
RECIPIENTS IS PROHIBITED
Do not remove this notice
Properly destroy or return documents when no longer needed**

- (3) The previous two statements must be **prominently** labeled in bold type in a size appropriate for the document or portable electronic data storage device or both, if applicable. On a set of construction drawings, for example, the statements must be in a minimum of 14 point bold type or equivalent.

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

- g. PBS contracting officers (COs), both realty and nonrealty, must insert the following contract clause¹ into (1) all solicitations containing SBU building information (including Solicitations for Offers (SFOs)); and (2) contracts and/or final leases that may contain, require access to, or cause the generation of SBU building information. Examples of such contracts are A-E design and construction contracts, and related professional service contracts such as construction manager as agent (CMA) and commissioning agent (CxA). When this clause is used, the CO must include instructions in the scope of work of the solicitation if contractors may be required to mark documents as SBU. COs must take appropriate action when they become aware that contractors have not fulfilled contractual obligations regarding the protection of SBU building information. Such action may include an investigation, referring the contractor for suspension or debarment proceedings, and/or terminating the contract for default. COs should document a contractor's failure to fulfill contractual obligations regarding the protection of SBU building information in performance assessment reports.

[Begin clause]

Safeguarding and Dissemination of Sensitive But Unclassified (SBU) Building Information

This clause applies to all recipients of SBU building information, including offerors, bidders, awardees, contractors, subcontractors, lessors, suppliers, and manufacturers.

(a) *Marking SBU.* Contractor-generated documents that contain building information must be reviewed by GSA to identify any SBU content, before the original or any copies are disseminated to any other parties. If SBU content is identified, the contracting officer may direct the contractor, as specified elsewhere in this contract, to imprint or affix SBU document markings to the original documents and all copies, before any dissemination.

(b) *Authorized recipients.* Building information considered SBU must be protected with access strictly controlled and limited to those individuals having a need to know such information. Those with a need to know may include Federal, State, and local government entities, and nongovernment entities engaged in the conduct of business on behalf of or with GSA. Nongovernment entities may include architects, engineers, consultants, contractors, subcontractors, suppliers, and others submitting an offer or bid to GSA or performing work under a GSA contract or subcontract. Contractors must provide SBU building information when needed for the performance of official Federal, State, and local government functions, such as for code compliance reviews and for the issuance of building permits. Public safety entities such as fire and utility departments may require access to SBU building information on a need to know basis. This clause must not prevent or encumber the dissemination of SBU building information to public safety entities.

(c) *Dissemination of SBU building information:*

(1) *By electronic transmission.* Electronic transmission of SBU information outside of the GSA firewall and network must use session (or alternatively file encryption). Sessions (or files) must be encrypted with an approved NIST algorithm, such as Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES), in accordance with Federal Information Processing Standards Publication (FIPS

¹ This clause has been proposed for inclusion in GSAM Section 504.

PUB) 140-2, Security Requirements for Cryptographic Modules. Encryption tools that meet FIPS 140-2 are referenced on the NIST web page found at the following URL: <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm>. All encryption products used to satisfy the FIPS 140-2 requirement should have a validation certificate that can be verified at the following URL: <http://csrc.nist.gov/groups/STM/cmvp/validation.html#02>. (Not all vendors of security products that claim conformance with FIPS 140-2 have validation certificates.) Contractors must provide SBU building information only to authorized representatives of State, Federal, and local government entities and firms currently registered as "active" in the Central Contractor Registration (CCR) database at www.ccr.gov that have a need to know such information. If a subcontractor is not registered in the CCR and has a need to possess SBU building information, the subcontractor shall provide to the contractor its DUNS number or its tax ID number and a copy of its business license.

(2) *By nonelectronic form or on portable electronic data storage devices.* Portable electronic data storage devices include but are not limited to CDs, DVDs, and USB drives. Nonelectronic forms of SBU building information include paper documents.

(i) By mail. Utilize only methods of shipping that provide services for monitoring receipt such as track and confirm, proof of delivery, signature confirmation, or return receipt.

(ii) In person. Contractors must provide SBU building information only to authorized representatives of State, Federal, and local government entities and firms currently registered as "active" in the CCR database that have a need to know such information.

(3) *Record keeping.* Contractors must maintain a list of the State, Federal, and local government entities and the firms to which SBU is disseminated under sections (c) (1) and (c) (2) of this clause. This list must include at a minimum (1) the name of the State, Federal, or local government entity or firm to which SBU has been disseminated; (2) the name of the individual at the entity or firm who is responsible for protecting the SBU building information, with access strictly controlled and limited to those individuals having a need to know such information; (3) contact information for the named individual; and (4) a description of the SBU building information provided. Once work is completed, or for leased space with the submission of the "as built" drawings, the contractor must collect all lists maintained in accordance with this clause, including those maintained by any subcontractors and/or suppliers, and submit them to the contracting officer. For federal buildings, final payment may be withheld until the lists are received.

(d) *Retaining SBU documents.* SBU building information (both electronic and paper formats) must be protected, with access strictly controlled and limited to those individuals having a need to know such information.

[If returning SBU documents to the CO is not allowed on a particular contract, remove the italicized language below from the clause, and capitalize the 'E' at the beginning of the applicable sentence.]

(e) *Destroying SBU building information.* SBU building information must be destroyed such that the marked information is rendered unreadable and incapable of being restored, or returned to the contracting officer, when no longer needed, in accordance with guidelines provided for media sanitization within Appendix A of NIST Special Publication 800-88, Guidelines for Media Sanitization, available at http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf. *If SBU*

building information is not returned to the contracting officer, examples of acceptable destruction methods for SBU building information are burning or shredding hardcopy; physically destroying portable electronic storage devices such as CDs, DVDs, and USB drives; deleting and removing files from electronic recycling bins; and removing material from computer hard drives using a permanent-erase utility such as bit wiping software or disk crushers.

(f) *Notice of disposal.* The contractor must notify the Contracting Officer that all SBU building information has been destroyed, *or returned to the Contracting Officer*, by the contractor and its subcontractors or suppliers in accordance with section (e) of this clause, with the exception of the contractor's record copy. This notice must be submitted to the contracting officer at the completion of the contract in order to receive final payment. For leases, this notice must be submitted to the Contracting Officer at the completion of the lease term.

(g) *Incidents.* All improper disclosures of SBU building information must be immediately reported to the contracting officer at _____<insert address and contact information>____. If the contract provides for progress payments, the contracting officer may withhold approval of progress payments until the contractor provides a corrective action plan explaining how the contractor will prevent future improper disclosures of SBU 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.

(h) *Subcontracts.* The Contractor must insert the substance of this clause in all subcontracts.

[End of clause]

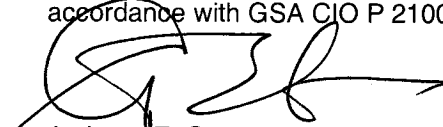
9. Limiting dissemination to authorized recipients. SBU building information must be disseminated only after it is determined that the recipient is authorized to receive it. The criterion to determine whether a recipient is authorized to receive SBU building information is “*need to know.*”
 - a. Federal, State, and local government entities and utilities. GSA must provide SBU building information as needed for the performance of official Federal, State, and local government functions, such as for code compliance reviews and for the issuance of building permits. Public safety entities such as fire departments may require access to SBU building information on a need to know basis. This Order must not prevent or encumber the dissemination of SBU building information to public safety entities. Utility companies may require access to SBU building information for the performance of work on GSA-controlled space on a need to know basis.
 - b. Nongovernment entities. PBS disseminators are reminded of the FAR 5.102(a)(4) requirement to use the FedTeDS website for posting any solicitations containing SBU building information to monitor access and distribution if the action was synopsisized through the Governmentwide Point of Entry or FedBizOpps (FBO). Unless the action is exempt under FAR 4.1102, all PBS disseminators are responsible for verifying that the recipient firm is currently registered as “active” in the CCR database before releasing any SBU building information to that nongovernment entity.
10. Electronic transmission of SBU building information. PBS associates, who electronically transmit SBU building information outside of the GSA firewall, must encrypt the data with an approved NIST algorithm, such as Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES), in accordance with Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules. PBS associates working within the GSA network, and transmitting to other GSA associates, may transmit SBU building information using standard

operating procedures. ("Within the GSA network" means inside the firewall, including Citrix and GSA VPNs.)

11. Dissemination of SBU building information in non-electronic form or on portable electronic data storage devices.² Portable electronic data storage devices include but are not limited to CDs, DVDs, and USB drives. Non-electronic forms of SBU building information include paper documents.
 - a. By mail. Utilize only methods of shipping that provide services for monitoring receipt such as track and confirm, proof of delivery, signature confirmation, or return receipt.
 - b. In person. PBS associates must provide SBU building information only to authorized representatives of Federal, State, and local government entities and CCR-registered firms that have a need to know such information.
12. Retaining SBU building information. PBS associates must not take SBU building information outside of GSA facilities except as necessary for the performance of a GSA project. If a PBS associate takes SBU building information outside of a GSA facility, access to the information must be limited to those with a need to know. Such information must be returned to a GSA facility or destroyed when no longer needed for the performance of a GSA project. PBS associates must not retain SBU building information on computers or removable electronic media that are not owned by GSA.
13. Destroying SBU building information. Sanitization and disposal of SBU building information contained in GSA storage media and devices must be accomplished in accordance with CIO IT Security 06-32, Media Sanitization Guide, upon contract closeout or whenever the SBU information is no longer needed. GSA paper or hardcopy documents containing SBU building information must be properly destroyed or disposed of in recycling bins specifically designated for sensitive information.
14. Freedom of Information Act (FOIA) requests. SBU markings do not control the decision of whether to disclose or release the information to the public, such as in response to a FOIA request. Because of security concerns, SBU building information must not be disclosed in accordance with a FOIA request without a thorough analysis of the security implications and any potentially applicable exemptions under the FOIA. Any determination to disclose SBU building information in accordance with a FOIA request must be made by the PBS ARA or the PBS Deputy Commissioner, after consultation with the servicing legal office.
15. Reporting incidents of concern. Any offense that may have been committed against property owned or occupied by the Federal Government must be reported to the Department of Homeland Security (DHS) Federal Protective Service (FPS) at 877-4FPS-411 for investigation.

PBS associates must report to a PBS management official any known or suspected dissemination of SBU building information to unauthorized users. The PBS management official must immediately report the incident to the GSA OIG for investigation if warranted.

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 GSA CIO P 2100.1, Information Technology (IT) Security Policy Order.



Anthony E. Costa
Acting Commissioner
Public Buildings Service

² Not applicable to any solicitation containing SBU building information that must be posted to FedTeDS if synopsis on FBO per FAR 5.102(a) (4).

Attachment 1

Examples of Sensitive But Unclassified Building Information

The following are examples of SBU building information and nonsensitive information:

1. SBU building information may be contained in any document (including drawings, specifications, virtual modeling, reports, studies, analyses) with information pertaining to:
 - a. Location and details of secure functions or space in a building. Examples:
 - Judges' parking, chambers, and libraries.
 - Prisoner or judges' secure circulation paths or routes (both vertical and horizontal).
 - Secure elevator locations.
 - Detention or holding cells.
 - Sally ports.
 - Security areas.
 - Child Care Centers.
 - Major computer processing areas or other client-sensitive processing and communications areas (such as major photo or computer facilities).
 - b. Location and details of secure functions or secure space. Examples:
 - Heating, ventilation, air conditioning (HVAC).
 - Information technology (IT) systems.
 - Air intake vents.
 - Water sources.
 - Gas lines.
 - Plumbing lines.
 - Building automation systems.
 - Power distribution systems.
 - Telephone and cable distribution systems.
 - Emergency generation equipment.
 - Uninterrupted power sources (UPS).
 - Security and fire alarm systems.
 - Routes and annunciation panels.
 - c. Location and type of structural framing for the building, including any information regarding structural analysis. Examples:
 - Progressive collapse.
 - Seismic.
 - Building security.
 - Blast mitigation.
 - Counterterrorism methods taken to protect the occupants and the building.

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

- Camera locations.
- Nonpublic security guard posts (i.e., number, location, operations).

2. Nonsensitive information. Any document (including drawings, specifications, virtual modeling, reports, studies, analyses) that does not contain information considered a security risk, or in which specific SBU building information, as identified above, has been redacted before release or presentation to the public, is not SBU. Examples include:

- Interior and exterior photographs limited to publicly accessible space or those that have been cleared for publication by GSA or the agency responsible for the space.
- Models.
- Building elevations.
- Sketches, tentatives, renderings, conceptual and space-planning drawings, floor plans or layouts.
- Building footprint and massing plans.
- Building drawings with SBU information redacted or shown as generic space.