Manual Guide - Information Security CDC-02
Date of Issue: 07/22/2005
Proponents: Office of Security and Emergency Preparedness

SENSITIVE BUT UNCLASSIFIED INFORMATION

Sections

I. PURPOSE
II. BACKGROUND
III. SCOPE
IV. ACRONYMS AND DEFINITIONS
V. POLICY
VI. PROCEDURES
VII. RESPONSIBILITIES
VIII. REFERENCES

Exhibit 1: Common Information Types with Sensitivity Guidance

Exhibit 2: Summary Listing of Common Information Types

I. PURPOSE

The purpose of this document is to provide policy and procedures to the Centers for Disease Control and Prevention[1] (CDC) that allow for the accomplishment of our public health service mission while safeguarding the various categories of unclassified data and document information that, for legitimate government purposes and good reason, shall be withheld from distribution or to which access shall be denied or restricted.

II. BACKGROUND

There are various categories of information, data and documents that are sensitive enough to require protection from public disclosure–for one or more reasons outlined under the exemptions of the Freedom of Information Act but may not otherwise be designated as national security information.

III. SCOPE

This policy applies to all individuals, employees, fellows, attached uniform service members, Public Health Service Commissioned Corps, Department of Defense employees and service members, contractors and subcontractors working at CDC, or under the auspices thereof.

IV. ACRONYMS AND DEFINITIONS

A. For the purposes of this policy, the following acronyms apply.

1. **CARI:** Contractor Access Restricted Information
2. **CSASI:** Computer Security Act Sensitive Information
3. **CUI:** Controlled Unclassified Information

4. **DCO:** document control officer
5. **DEA-S:** Drug Enforcement Agency Sensitive
6. **DOD:** Department of Defense
7. **DOE-OUO:** Department of Energy Official Use Only
8. **DOS-SBU:** Department of State Sensitive But Unclassified
9. **EO:** Executive Order
10. **FOIA:** Freedom of Information Act
11. **FOUO:** For Official Use Only
12. **GSA:** General Services Administration
13. **GSA-SBU-BI:** GSA Sensitive But Unclassified Building Information
14. **HHS:** Department of Health and Human Services
15. **ITAR:** International Traffic in Arms Regulations
16. **LES:** Law Enforcement Sensitive
17. **LOU:** Limited Official Use
18. **OSEP:** Office of Security and Emergency Preparedness
19. **OSPI:** Operations Security Protected Information
20. **PAPI:** Privacy Act Protected Information
21. **PHS:** Public Health Service
22. **PROPIN :** proprietary information
23. **SASI:** Select Agent Sensitive Information
24. **SBU:** Sensitive But Unclassified
25. **SDD:** Security and Drug Testing Program Division
26. **SNM:** Special Nuclear Material
27. **UCNI:** Unclassified Controlled Nuclear Information

B. For the purposes of this policy, the following definitions apply.

1. Sensitive But Unclassified

This designation is applied to unclassified information that may be exempt from mandatory release to the public under FOIA. SBU is the formal designation for information that by law or regulation requires some form of protection but is outside the formal system of classification, as in accordance with Executive Order 12958, as amended. There are currently 13 types or categories of SBU, established to allow for specific administrative methods and procedures: CSASI, CARI, CUI, DEA-S, DOE-OUO, DOS-SBU (formerly known as LOU), FOUO, GSA-SBU-BI, LES, OSPI, PAPI, SASI, and UCNI.

2. Computer Security Act Sensitive Information

"Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, USC (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." Reference Public Law 100-235, The Computer Security Act of 1987, which is concerned with protecting the availability and integrity as well as the confidentiality of information.

3. Contractor Access Restricted Information

Unclassified information that involves functions reserved to the federal government as vested by the Constitution as inherent power or as implied power as necessary for the proper performance of its duties. In many instances, CARI prevents contractors from making decisions that would affect current or future contracts and procurement procedures, primarily during pre-award activities. CARI maximizes competition for government requirements and encourages absolute integrity in all dealings with the private sector while promoting economy, efficiency and effectiveness. See Acquisition Management Policy CDC-10, Procurement Integrity Restrictions.

4. Controlled Unclassified Information

DOD unclassified information that requires application of controls and protective measures for a variety of reasons other than national security information (that has been classified in accordance with EO 12958, as amended, or any precursory executive orders). Policy and procedures for CUI are found in and are in accordance with DOD Regulation 5200.1-R, The Information Security Program.

5. DEA Sensitive

DEA Sensitive is unclassified information that is originated by DEA and requires protection against unauthorized disclosure in order to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. The administrator and certain other officials of the DEA have been authorized to designate information as "DEA SENSITIVE."

6. Department of State Sensitive But Unclassified

Unclassified information that originated within the Department of State which warrants a degree of protection or administrative control and meets the criteria for exemption from mandatory public disclosure under FOIA. Prior to 26 January 1995, this information was designated and marked LOU. The LOU designation will no longer be used.

7. DOE Official Use Only

The Department of Energy designation for information that is sensitive but unclassified and is, or should be, exempt from public release under FOIA.

8. Export Controlled Information (or material)

Information or material that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State. This pertains to items controlled by the ITAR, or the Department of Commerce for items controlled by the Export Administration Regulations (EAR). Export Controlled Information must be controlled as “Sensitive But Unclassified” information and marked accordingly. A large, frequently updated database of information on export administration regulations is available at http://www.access.gpo.gov/bis/ear/ear_data.html.

9. The Arms Export Control Act

Act which regulates the export of defense articles and services. Such exports may be licensed only if their export will strengthen United States national security, promote foreign policy goals, or foster world peace. The Arms Export Control Act is administered by the Department of State, Center for Defense Trade Controls, through the ITAR and the United States Munitions List (defense articles that require a license prior to export).

10. The Export Administration Act

Act which regulates the export of dual-use items (those that have both a military and civilian use). Dual-use items that would make a significant contribution to the military potential of another country are on the Department of Commerce's Commodity Control List, and a license is required for their export. The Commodity Control List includes items from the Defense Department's Military Critical Technology List and technology that could support the proliferation of chemical, biological or nuclear weapons or missile technology. A recent study of illegal technology transfer operations directed against the United States identified 56 different end-user countries.

11. For Official Use Only

A designation that is applied to unclassified information that is exempt from mandatory release to the public under FOIA. FOIA specifies nine categories of information that can be withheld from public (see definition below). Information that is currently and properly classified can be withheld from mandatory release under the first exemption category (subparagraph (a) below). FOUO is applied to information which is exempt under one of the other eight categories.

12. Freedom of Information Act

This requires the release of publicly requested information with several exceptions:

(a) Information that is currently and properly classified.

(b) Information that pertains solely to the internal rules and practices of the agency and, disclosure would allow circumvention of agency regulations.

(c) Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

(d) Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.

(e) Intra-agency memoranda that are deliberative in nature—this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.

(f) Information for which the release could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

(g) Records or information compiled for law enforcement purposes that:

(1) could reasonably be expected to interfere with law enforcement proceedings;
(2) would deprive a person of a right to a fair trial or impartial adjudication;
(3) could reasonably be expected to constitute an unwarranted invasion of personal privacy of others;
(4) discloses the identity of a confidential source;
(5) discloses investigative techniques and procedures; or
(6) could reasonably be expected to endanger the life or physical safety of any individual.

(h) Certain records of agencies responsible for supervision of financial institutions.

(i) Geological and geophysical information concerning wells.

13. GSA Sensitive But Unclassified Building Information

Information concerning General Services Administration Public Building Services controlled space including owned, leased or delegated Federal facilities. GSA-SBU-BI includes building designs such as floor plans, construction plans and specifications, renovation/alteration plans, equipment plans and locations, building operating plans, information used for building services contracts and/or contract guard services, or any other information considered a security risk, such as, but not limited to:

(a) Locations of secure functions in the facility, such as VIP offices and conference rooms, security areas, childcare, major computer processing or equipment rooms;

(b) Location of all utilities, such as heating, ventilation, air conditioning, information technology systems, location of air intake vents, water sources, gas lines, plumbing lines, building automation systems, power distribution systems, emergency generation equipment, uninterruptible power sources, security and fire alarm systems/routes and annunciation panels;

(c) Location and type of structural framing for the building and any information regarding structural analysis, or building security and blast mitigation analysis and counter terrorism methods taken to protect the occupants and building; and

(d) Information regarding security systems or strategies of any kind (such as camera locations) or security guards (such as number and location). References: GSA PBS 3490.1 of March 8, 2002, GSA Order Safeguarding Sensitive Unclassified Information (ADM 1800.3B); Instructional Letter CIO IL-99-1, Safeguarding Sensitive Unclassified Information; and GSA Acquisition Manual (GSAM) (ADP P2800.12B).

14. Law Enforcement Sensitive

A designation and marking for records or information compiled for law enforcement purposes that the release of:

(a) could reasonably be expected to interfere with law enforcement proceedings;

(b) would deprive a person of a right to a fair trial or impartial adjudication;

(c) could reasonably be expected to constitute an unwarranted invasion of personal privacy of others;

(d) disclose the identity of a confidential source;

(e) disclose investigative techniques and procedures; or

(f) could reasonably be expected to endanger the life or physical safety of any individual.

15. Operations Security Protected Information

Unclassified information concerning CDC mission, functions, operations, or programs that require protection in the national interest, security or homeland defense as iterated in National Security Decision Directive 298, January 1988, which established a National Operations Security Program.

16. Privacy Act Protected Information

Information that if released could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals. Additional guidance may be found in the Privacy Act of 1974, 5 USC 552a, 45 CFR Part 5b, and in General Administration Policy CDC-63, Privacy Act.

17. Proprietary Information

Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.

18. Select Agent Sensitive Information

The portion of the National Laboratory Registration and Select Agent Program information that has been determined by the HHS Original Classification Authority to be sensitive but unclassified and is prohibited from public disclosure by Public Law 107-188, Public Health Security and Bioterrorism Preparedness and Response Act of 2002. See also 42 USC 247d-6b(d).

Classification Guidance:
HHS has classified the Select Agent Program electronic and document database. This database contains information concerning the possession, use, or transfer of select biological agents and toxins as required by 42 CFR Part 73 and 43 CFR 72.6. The Select Agent Program electronic and document database, and any portion of that database, which contains information concerning more than one entity, is classified as SECRET.

Any document that has been prepared using information from the Select Agent Program database, which identifies more than one entity as having a specific select agent or agents, is classified as SECRET.

Any document that has been prepared using information from the Select Agent Program database which identifies more than one entity as having an unspecified select agent or agents, is classified as CONFIDENTIAL.

A portion of the Select Agent Program database, or any document that has been prepared using information from the Select Agent Program database, which is limited to information received from one entity will be unclassified but will be protected to safeguard the public interest and marked as FOR OFFICIAL USE ONLY. It would be inappropriate to give such material to persons outside Federal agencies without the consent of a responsible HHS official.

Cover sheet marking for Select Agent Sensitive Information (SASI):
"This document is intended for the exclusive use of the recipient(s) named above. It may contain sensitive information that is protected, privileged, or confidential, and it should not be disseminated, distributed, or copied to persons not authorized to receive such information. If you are not the intended recipient(s), any dissemination, distribution, or copying is strictly prohibited. If you think that you have received this document in error, please notify the sender immediately and destroy the original."

19. Unclassified Controlled Nuclear Information

Unclassified information on aspects of security, including security plans, procedures, methods/measures, and equipment, for the physical protection of DOD SNM, equipment, and facilities. Information is designated DOD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security, by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DOD SNM, equipment, or facilities.

V. POLICY

All CDC employees and otherwise affiliated persons shall protect Sensitive But Unclassified information by following the procedures contained in this policy document and/or related policies of the CDC, HHS, Executive Orders, other presidential directives, United States Federal Court rulings, and applicable laws of the United States of America.

Policies and Procedures for the protection of National Security Information (Classified Information) are marked as Confidential, Secret, or Top Secret in accordance with Executive Order 12958, as amended, and can be found in other CDC and HHS documents (see section VIII. References of this policy for specific citations).

VI. PROCEDURES

A. Review and Approval of Information Prior to Public Release

A process has been established for review and approval of all information–including hard copies and digital publications–prior to its public release. The OSEP has appointed a DCO who is authorized to review and approve information for release and to clear policies and procedures for posting web site content. The DCO is further authorized to make sensitivity determinations ensuring that certain information is not for public release (subject to the FOIA officer), and that the information should be marked as SBU.

However, marking information SBU does not automatically qualify it for a public release exemption. If a public request for a SBU document is received, the information should be reviewed to determine if it actually qualifies for exemption. Moreover, the absence of the SBU or other related marking does not necessarily mean the information should be publicly released. Some types of records (e.g., most human resources and financial information) are not normally marked SBU but may still qualify for withholding under FOIA, unless otherwise authorized for release by the individual. Therefore, all information should be reviewed and approved prior to its public release.

To protect against the unauthorized disclosure of classified information, all CDC employees and otherwise affiliated persons are required to submit for sensitivity review any material intended for public release that might be based in any way on information learned through access to classified information. This requirement covers all written materials—including technical papers, books, articles, and manuscripts—lectures, speeches, films, and videotapes.

The requirement for a sensitivity review applies equally to hard-copy and electronic documents. Electronic documents that require sensitivity review include, but are not limited to, submissions to online publications, documents that are drafted or stored on a publicly accessible home page, and submissions to another Internet site, regardless of site or location.

For some persons with access to Sensitive Compartmented Information (SCI) or a DOD Special Access Program (SAP), the requirement for pre-publication review may extend to résumés and curriculum vitae that identify specific tasks performed while holding the clearance.

When any portion of the information proposed for disclosure "might" be covered by a signed nondisclosure agreement, CDC employees and otherwise affiliated persons may not take any steps toward public disclosure until receiving written permission to do so. This is a lifetime obligation that remains in effect as long as the information remains classified or sensitive.

The government may take control of all rights, title, and interest in any and all "royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms" of the nondisclosure agreement signed at the time of security clearance acceptance.

B. Pre-Publication Review of Web Site Content

Information on the Internet may be intended for a limited audience; however it actually becomes available to a world wide audience. The World Wide Web was not designed with security in mind, and unencrypted information is at high risk of compromise. CDC OCISO and ITSO guidelines take into account what security access controls, if any, are in effect for specific sites, the sensitivity of the information, and the target audience for which the information is intended.

Most types of SBU information (i.e., DOD Technical Information, FOUO information, export-controlled information, Unclassified Nuclear Information, and Privacy Act information) shall not go on a web site unless that site is protected by encryption. Decisions on the handling of proprietary or trade secret information in the private sector are made by the owners of that information.

SBU information is normally marked with a sensitivity indicator at the time it is created. However, the absence of any sensitivity marking is not a valid basis for assuming that information is non-sensitive. If information could be considered sensitive, it should first be seen by the DCO at the branch level.

CDC sensitivity determinations and classification decisions require that judgments consider the potential consequences of aggregation. The term "sensitive by aggregation" refers to the fact that information on one site may seem unimportant, but when combined with information from other web sites, it may form a larger and more complete picture that was neither intended nor desired. Similarly, the compilation of a large amount of information together on one site may increase the sensitivity of that information and make it more likely that site will be accessed by those seeking information that can be used against the government.

There are several common mistakes that people make when deciding what to put on a web site: ignoring the danger associated with personal data on the Internet; assuming that information is not sensitive because it is not marked with a sensitivity indicator; and underestimating the ease and potential significance of aggregation.

Personal information such as: addresses; telephone numbers, other than those readily available to the public; social security numbers; dates of birth; names of family members in biographic summaries, etc; could facilitate criminal, harassment, or terrorist activity against military personnel or government or defense contractor employees and should not be on the Internet.

C. Sensitivity/Classification Decision and Notification

The DCO shall issue a decision within 5 working days as to the sensitivity of information of a draft document. If a decision cannot be made, or if it is determined that the information should be classified, the document will be sent to either a security review panel at OSEP and/or forwarded to HHS/SDD for a classification determination. The originator will be promptly notified as to the status of the document, especially those documents that have been referred to the review panel or to HHS.

D. Appeal of Sensitivity/Classification Decision

Sensitivity determinations may be appealed by a formal written request from the originator through the affected center/office director and sent to the Director of OSEP for a final determination. Appeals regarding classification determinations must follow the formal Classification Challenge Procedures as specified per EO 12958, as amended; the ISOO Implementing Directive of September 2003; and the current HHS National Security Information Manual.

E. Types of Sensitive But Unclassified Information

Sensitive information consists of any information exempted from FOIA and includes, but is not limited to, information related to personnel, security, select agents, and HHS-designated critical national electronic surveillance systems.

Examples include, but are not limited to:

1. Personnel. General personnel information including: evaluation and performance data; security information, including background investigation results and adjudication, and infractions/incident reports; personal information when associated with an individual's work on topics where security is involved (e.g., names and details of those working with select agents, classified data, counterintelligence) or with those individuals who are authorized to have a level of access beyond the average CDC employee, contractor, or visitor.

2. Security. Facility blueprints and other detailed facility information, databases associated with the physical security system, vulnerabilities of such facilities or sensitive information, network security information, security procedures, access codes (combinations or passwords), badge design information, security audit results, physical security performance test results, results of response force exercises, incident reports and disciplinary actions, response force capabilities, and security plans.

3. Select Agents. Databases and lab records associated with the select agent program including, but not limited to, inventory databases and chain-of-custody

records; select agent transfer records; documentation associated with the unexpected results of an experiment, that if deliberately conducted would be prohibited by 9 CFR § 121.10; and information deemed too sensitive for public release by a review and approval panel.

F. SBU Mandatory Release Exemptions under the Freedom of Information Act (FOIA)

Information, in either electronic or hard copy form, determined to be sensitive but unclassified should fall within one or more of the eight FOIA exemption categories identified in Section IV (FOIA definition) to be exempt from mandatory release to the public.

G. SBU Personnel Access Requirements

Access to Sensitive Information. Sensitive information should only be released to authorized employees who have a specific job-related need-to-know for that information. The final responsibility for determining whether an individual has a need for access to sensitive information should be determined by the individual who has authorized possession, knowledge, or control of the information. Individuals responsible for sensitive information should be authorized to convey such information to others who have an official need-to-know.

H. SBU Safeguarding / Storage Requirements

1. Protection of Sensitive But Unclassified While In Use. Reasonable precautions should be taken to prevent access to sensitive information by persons who do not require the information to perform their jobs (e.g., sensitive documents should neither be read in a public place, nor taken home).

2. Storage Rules for Sensitive But Unclassified. Sensitive information, both in hard copy and electronic form, should be physically protected and should be stored in limited areas. Exclusion areas and special exclusion areas are also acceptable storage locations, but high containment laboratories should only be used as storage areas for sensitive information when absolutely necessary. Storing sensitive information in a property protection area or a public area is only acceptable if additional protections are taken to increase protection to a level comparable to that in a limited area.

All sensitive information existing in hard copy should be stored within a locked container in a limited or exclusion area, an access controlled electronic environment, or be under the physical control of an authorized individual. When limited or exclusion areas are not available, for instance when an individual is traveling within the United States, a locked container within a locked room will suffice (e.g., locked briefcase or suitcase within a locked hotel room or vehicle). Sensitive information should not be taken outside the United States.

Information handled electronically and transmitted over the network is at a higher risk of being released or altered. Sensitive information stored on the CDC network should be protected at a level that can ensure that only those who are authorized to view the information are allowed access (e.g., machine-generated

passwords, encryption). The CDC network systems should maintain a high level of electronic protection (e.g., firewalls, intrusion detection, defense-in-depth, isolation of sensitive information, good practices network administration) to ensure the integrity of sensitive information and to prevent unauthorized access into these systems. Regular review of the protection methods used and system auditing are also critical to maintain protection of these systems.

The physical elements of the network systems which store and transmit sensitive information or that have direct access to sensitive information should be secured within a Limited Area or Exclusion Area. The more central the information resource is (e.g., a network or security system control room) the higher the level of access control that should be applied.

I. SBU Marking Requirements

1. Marking Rules for Sensitive But Unclassified. Information that has been determined to be SBU should be designated as "Sensitive But Unclassified" with the appropriate markings and labels.

2. Documents. Documents containing sensitive information should be covered with a "Sensitive But Unclassified" cover page, and the outside of the back cover should be marked "Sensitive But Unclassified."

Internal pages of the document should be marked "Sensitive But Unclassified" at the top and bottom of each page in letters clearly distinguishable from the text. The acronym SBU may be used when space does not permit spelling out "Sensitive But Unclassified."

The first page should contain the following statement at the lower left hand corner, and should be completed with the applicable FOIA exemption number(s).

Sensitive But Unclassified (SBU)

This document contains information that may be exempt from public release under the Freedom of Information Act (FOIA) (5 U.S.C. 552), exemption(s) _____ apply. Approval by the Centers for Disease Control and Prevention Document Control Officer (OSEP) and the CDC FOIA Officer, prior to public release via the FOIA Office is required.

3. Electronic Media. Electronic media containing sensitive information should be labeled "Sensitive But Unclassified." The label should be plainly visible and should be applied in a way that it does not interfere with the drive mechanism. Electronic media includes magnetic tape reels, disk packs, diskettes, compact discs, removable hard disks, disk cartridges, optical disks, paper tape, reels, magnetic cards, tape cassettes and micro-cassettes, videotapes, and any other device on which data is stored and which normally is removable from the system by the user or operator. The outer covering for any of the above removable storage media should also be marked "Sensitive But Unclassified."

Videotapes should also contain “Sensitive But Unclassified” at the beginning and end of the played video, if possible. Audible cassettes, if possible, should contain an audible statement at the beginning and end of the played portion, which informs the listener that the tape contains sensitive unclassified information.

4. Blueprints, Engineering Drawings, Charts, and Maps. Blueprints, engineering drawings, charts, and maps containing sensitive information should be marked “Sensitive But Unclassified - Building Information” or "SBU-BI" at the top and bottom of each page. If the blueprints, drawings, charts, or maps are large enough that they are likely to be rolled or folded, “Sensitive But Unclassified - Building Information” should be placed to be visible when the item is rolled or folded.

5. Photographs and Negatives. Photographs containing sensitive information should be marked “Sensitive But Unclassified” on the face, if possible. If this cannot be done, the marking should be placed on the reverse side. Negatives, positives, or other film containing sensitive information should be marked “Sensitive But Unclassified” on the film itself if possible, otherwise protected inside a marked container.

J. Reproduction of Sensitive But Unclassified

SBU Documents may be reproduced without the permission of the originator to the extent necessary to carry out official CDC activities. Copies should be protected in the same manner as originals. In the event of a copy machine malfunction, the copy machine should be cleared and all paper paths checked for papers containing sensitive information.

K. SBU Transfer Requirements

1. Communicating Sensitive Information. Sensitive information may be communicated in the following ways:

- from person to person in direct contact with one another;
- over a land-line telephone;
- via first class, priority, or overnight mail;
- via fax machine;
- via e-mail to and from CDC e-mail addresses ([...]@cdc.gov) that reside completely within the CDC network; or
- via e-mail to and/or from an e-mail address outside of the CDC network, provided that the sensitive data is encrypted and authenticated.

2. Discussing Sensitive Information via Telephone or Video Conference. Although sensitive information may be discussed on landline telephones, sensitive information should not be discussed on cellular phones. Sensitive information should not be transmitted via open network communication channels, including online video conferencing unless such a conference is held on a restricted network.

3. Mailing of Sensitive Information. Transmission of sensitive information should be done in a manner that informs those with a need-to-know of the level of sensitivity while not advertising the fact to the general public. It is also important to use a reliable means of shipping. These considerations help to avoid unauthorized disclosure or dissemination of sensitive information.

4. Internal Mail. Before transmitting sensitive information through the CDC internal mail, the information should have appropriate markings and cover sheet and be placed in a "Sensitive But Unclassified" envelope.

5. External Mail. Sensitive information sent outside CDC premises should be transmitted via first class mail, priority, or overnight mail. The outer wrapping should not be marked in a manner that would reveal the contents of the envelope or package to unauthorized personnel.

6. Faxing of Sensitive But Unclassified Information. Prior to faxing sensitive information, the sender should confirm that an authorized person will be present to accept the transmittal at the receiving end, or the sender should verify that the receiving facility is protected in a manner sufficient to preclude unauthorized access to the transmitted material.

7. Electronic Transmission. Sensitive information should be encrypted and authenticated if it is sent from the CDC network to an unsecured (non-CDC) network. Sensitive information should never be communicated over wireless technologies, such as cellular or cordless telephones, or wireless data devices (e.g., Blackberries).

L. SBU Disposal / Destruction Requirements and Methods

Destruction of Sensitive Information

Sensitive information should be destroyed by shredding or burning; paper containing sensitive information should not be recycled.

Deleting, erasing, or formatting will not sufficiently remove sensitive information from electronic storage formats. Instead, files should be removed by using multiple passes (10 times minimum) of a hard drive wiping program.

Electronic or removable media should be physically damaged to the point of inoperability, via shredding, degaussing, melting, or other such methods before disposal.

M. Enforcement

A violation of this policy may be cause for administrative action, including, but not limited to, removal from employment or discharge from USPHS Commissioned Corps. Violations of this policy may also result in civil and criminal penalties, including fines and imprisonment, under the laws of the United States.

N. Information Contact

For additional information about this policy, or to submit a document for sensitivity review or classification determination, contact the OSEP Document Control Officer at 404-639-7650.

VII. RESPONSIBILITIES

A. OSEP responsibilities regarding sensitive but unclassified information

CDC OSEP shall appoint one or more DCO(s) to implement this policy and procedures. The Director of OSEP shall form an appeal board as needed to render timely judgments concerning appeals to sensitivity determinations. The Director shall forward challenges to classification decisions according to the DHHS Manual on National Security Information.

B. DCO(s) responsibilities regarding sensitive but unclassified information

DCO(s) shall review all submitted materials and render a sensitivity determination or process same for a national security information classification decision in accordance with this policy and applicable other laws, orders, rules and regulations. Sensitivity determinations and classification decisions and notification shall be documented and in a written form. Files will be maintained in accordance with the CDC Records Control Schedule.

C. Supervisors' and Managers' responsibilities regarding sensitive but unclassified information

Supervisors and managers shall ensure that only authorized employees have access to SBU information. They shall annually, and more often as necessary, inform their employees of the need to protect SBU information and of the requirement to have all documents that they create that may contain SBU sent to the DCO(s) for a sensitivity determination. They shall enforce the procedures of this policy among their employees and within the work spaces for which they are responsible. Supervisors shall report suspected or known violations of this policy or procedures to the DCO(s) as soon as possible.

D. Employees' and Affiliated Persons' responsibilities regarding sensitive but unclassified information

Employees and affiliated persons shall become knowledgeable of this policy and procedures. They shall comply with the requirements as herein established.

E. CDC FOIA Officer responsibilities regarding sensitive but unclassified information

CDC FOIA Officer shall obtain a sensitivity determination or classification decision prior to final FOIA decision to release or deny CDC records.

F. CDC OCISO responsibilities regarding sensitive but unclassified information

CDC OCISO shall provide advice, assistance, policy and technical guidance on information systems security, with emphasis on FISMA 2002, and the Computer Security Act of 1987.

VIII. REFERENCES

A. Arms Export Control Act
B. CDC-3, Protection of Information Resources, April 10, 2002
C. CDC-5, Classified Material, April 10, 2002
D. CDC-8, Employee Use of CDC Information Technology Resources, June 9, 1999
E. CDC-10, Procurement Integrity Restrictions, February 21, 2004
F. CDC-18, Interim Clearance of Information Products Disseminated Outside CDC for Public Use, June 21, 2005
G. CDC-63, Privacy Act, November 30, 2000
H. CDC-78, Freedom of Information Act, March 9, 2002
I. CDC-83, Export Controls for Biological, Chemical, and Related Technical Data and Equipment, June 6, 1998
J. CDC-90, Federal Advisory Committee Meeting Minutes, December 21, 2000
K. CDC-102, CDC/ATSDR Policy on Releasing and Sharing Data, April 16, 2003
L. Department of Commerce's Commodity Control List
M. Department of Defense Military Critical Technology List
N. Executive Order 12731, "Principles of Ethical Conduct For Govenment Officers and Employees"
O. Executive Order 12600, Predisclosure Notification Procedures for Confidential Commercial Information
P. Executive Order 12958, Classified National Security Information
Q. Executive Order 13292, National Security Information
R. Export Administration Regulations (EAR)
S. Freedom of Information Reform Act of 1986 as Amended.
T. GSA PBS 3490.1 March 8, 2002, GSA Order Safeguarding Sensitive Unclassified Information (ADM 1800.3B)
U. GSA Instructional Letter CIO IL-99-1, Safeguarding Sensitive Unclassified Information
V. GSA Acquisition Manual (GSAM) (ADP P2800.12B).
W. International Traffic in Arms Regulations (ITAR)
X. National Security Decision Directive (NSDD) 298, January 1988, National Operations Security (OPSEC) Program
Y. Public Law 107-188 Public Health Security and Bioterrorism Preparedness Response Act of 2002
Z. Public Law 107-347 E-Government Act of 2002; Federal Information Systems Management Act
AA. Public Law 100-235 Computer Security Act of 1987

Exhibit I

CDC Common Information Types with Sensitivity Guidance

Overview

This document is part of CDC's information and security categorization guidance. It was created to assist the agency and its programs in their efforts to comply with Federal information security management regulations and supporting National Institute of Standards and Technology (NIST) standards. This document outlines categories of commonly used agency information, known as information types. This document also provides guidance on the content and general sensitivity of each information type and, in cases where information may be deemed sensitive, identifies corresponding Freedom of Information Act (FOIA) exemptions.

How to Use This Document

The purpose of this document is to provide information owners with a standardized listing of CDC-specific information types and to assist in the identification of potentially sensitive data. The information types described in this guide are applicable across all mission areas and apply to both hardcopy documents and computerized information systems. Typically, hardcopy information is assigned a sensitivity or confidentiality rating that indicates to users how the document must be accessed, stored, and controlled. Information used by computer systems may also be assigned a confidentiality rating but will have additional requirements for integrity and availability. In the case of information systems, these requirements form the security categorization rating for the system and relate directly to the protective controls required for safe and effective operation.

Information Sensitivity Ratings at CDC

The majority of information managed by CDC consists of public (non-sensitive) data. However, CDC also handles Sensitive but Unclassified (SBU) information and some National Security (Classified) materials. These designations are fully defined in CDC Classification Policies but are briefly described here for reference. Note: In the event of any discrepancy, CDC Classification Policies should be considered authoritative.

Classified information is information that has been determined, pursuant to Executive Order or law, to require protection against unauthorized disclosure. This information is typically associated only with national security interests and will be marked accordingly. When in doubt regarding the nature of a given data set or system, information owners should refer to NIST SP 800-59, "Guideline for Identifying an Information System as a National Security System" and should contact the Chief Information Security Officer (CISO).

Any other information, the unauthorized release of which could cause harm to the agency, its mission, employees, constituents, the public, or the national interest, *and* which meets one or more FOIA exemptions or qualifies for non-disclosure under some other protective statute, should be considered SBU. SBU is the formal designation for information that by law or regulation requires some form of protection but is outside the

formal system of classification, as in accordance with Executive Order 12958, as amended.

Information that is identified as neither Classified nor SBU is considered public.

Please note that this guidance applies only to agency public and SBU information. Please refer to Information Resources Management Policy CDC-05 for guidance on classified data.

The FOIA Process and Suggested Exemptions

FOIA allows the public to request a wide range of information from Federal agencies. In order to protect sensitive information, FOIA provides nine exemptions that can be used to prevent mandatory release. There are several laws, in addition to FOIA, that may specifically block the disclosure of certain information types. By definition, information that does not qualify under FOIA exemptions or other statutory protections cannot be considered sensitive.

Information owners should consider the applicability of the suggested exemptions defined in the table below when labeling or responding to requests for sensitive data. Please note that only the agency FOIA officer can officially assign exemptions or deny FOIA requests. Even then, some or all information related to a request may be released through departmental appeal or legal proceedings. The suggested exemptions are provided as a guide to allow information owners to better understand and communicate the sensitivity of their information and IT systems. Please consult with the CDC FOIA Officer for a complete listing of FOIA exemptions.

Understanding the Common Information Types Table

As noted above, the information types and sensitivity guidance provided in this document cover only public and SBU information. The table below is comprised of four columns. Columns 1 and 2, *'Information Type'* and *'Description and Examples,'* provide the name and description of each information type. Column 3, *'Potentially Sensitive?'* indicates the typical sensitivity level of the information type as follows:

- Yes – Information of this type is usually considered to be sensitive. All information types marked as sensitive will have one or more suggested exemptions in Column 4. Information owners should consult CDC policy guidance on the appropriate labeling and information management procedures required for this type of information. Please see Appendix A – References below for more information.

- Conditional – Information of this type is generally considered non-sensitive, but selected portions of the data may, in fact, require additional protection – for example: most portions of a facility plan may be publicly releasable, whereas detailed information regarding certain laboratories may necessitate added protection. In these cases, information owners should identify the sensitive content and consider segregating this data or raising the sensitivity level for all of the information to the level required by the most sensitive parts.

- No – Information of this type is generally considered to be non-sensitive (Public).

Lastly, Column 4, *'Potential Exemptions,"* provides information on FOIA exemptions and/or other statutes that may potentially be used to protect sensitive information from mandatory disclosure.

CDC Common Information Types

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Health Information and Mission Support			
Healthcare Information	Covers non-sensitive and non-proprietary information related to medical products, procedures, drugs, and tests.	No	
Public Health Data and Statistics	De-identified health information and/or information of sufficiently broad detail to prevent the identification of specific individuals through association or deduction.	No	

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Non-Public Health Data and Statistics (with Personal Identifying Information)	Data obtained from individuals, organizations, or other agencies under an Assurance of Confidentiality that contains either: 1) Personally identifying information including one or more of the following: name, home address and phone number, social security number, marital status, legitimacy of children, welfare payments, family fights and reputation, medical condition, date of birth, religious affiliation, citizenship data, genealogical history establishing membership in a Native American Tribe, criminal history records (commonly referred to as "rap sheets"), incarceration of United States citizens in foreign prisons, sexual inclinations or associations, and financial status 2) Information granular enough to potentially identify an individual through the information given or through association with other available information (small cell size)	Yes	FOIA Exemption 3: Public Health Service Act – Sections 301 and 308(d): Assurance of Confidentiality Also: Privacy Act – Based on the nature and function of the system in question and the scope of the information request Note: In 1984, Congress explicitly provided that the Privacy Act is not a statute covered under Exemption 3 and therefore cannot be cited under FOIA.
Mission Support	Covers the dissemination and exchange of information between the Federal Government, citizens, and stakeholders in direct support of mission services, public policy, and/or national interest. Includes official public communications, outreach, constituent service, and the general exchange of non-sensitive information.	No	

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Incident Investigation and Response			
Public Emergency Response Management	Covers information regarding agency strategies, capabilities, procedures, and resources for identification, monitoring, and response to public health emergencies, disasters, and/or other crises.	Conditional	
Investigative Activities	Covers information gathered during, and/or related to, ongoing internal and external law enforcement investigations where that information: (A) could reasonably be expected to interfere with enforcement proceedings; (B) would deprive a person of a right to a fair trial or an impartial adjudication; (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (D) could reasonably be expected to disclose the identity of a confidential source; (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; or (F) could reasonably be expected to endanger the life or physical safety of any individual. In this context “law enforcement” includes criminal, civil and administrative / regulatory proceedings.	Yes	FOIA Exemption 7(A) – While an investigation is pending – other exemptions or Exemption 7 subparts must be used if the information remains sensitive following enforcement procedures Also: FOIA Exemption 2 – Risk of Circumvention FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 – When dealing with events and information related to select agents and toxins and the Strategic National Stockpile.

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Strategic National Stockpile	Covers information relating to the locations of US pharmaceutical stockpiles	Yes	FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 Also: FOIA Exemption 2 – Risk of circumvention may be used to protect information regarding specific contents.

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Select Agents and Bioterrorism			
Select Agents	Covers information about the registration and transfer of Select Agents and Toxins, including the identity and location of specific registered persons.	Yes	FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 Also: FOIA Exemption 2 – Risk of circumvention may be used when dealing with safeguards, controls, and/or physical or electronic vulnerability assessments related to select agents.
Bioterrorism Monitoring and Surveillance Activities	Covers information related to the systems, processes, procedures, techniques, and algorithms used to monitor for signs of bio-terrorist activity and events.	Yes	FOIA Exemption 2 – Risk of Circumvention Also: FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 – when dealing specifically with Select Agents and Toxins

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Bioterrorism Events / Suspected Events and/or Response	Covers ongoing investigative / evidentiary information and other sensitive details surrounding an event or suspected event and response operations. Note that protection under Exemption 7(A) is lost after enforcement procedures are completed and sensitive information must be protected under other exemptions or other exemption 7 subparts.	Yes	FOIA Exemption 7(A) – while an investigation is pending, other Exemption 7 subparts during and after enforcement procedures are complete. Also: FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 – when dealing with Select Agents and Toxins. FOIA Exemption 4 – If dealing with information that may expose the trade secrets or proprietary information of an entity supplied during the investigation. FOIA Exemption 6 and/or Exemption 3: Public Health Service Act – Section 308(d): Assurance of Confidentiality – If dealing with personal identifying information (victims, decontamination, follow-up, etc.)

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Third Party Confidential Information			
Third Party Trade Secrets, Confidential, and Proprietary Information	Covers information supplied to the government by a third party that includes “trade secrets” or other privileged or confidential information, such as product manufacturing and design data, business sales statistics, research data, technical designs, currently unannounced and future products, customer and supplier lists, names of consultants and subcontractors, raw research data used to support a pharmaceutical drug's safety and effectiveness, information regarding an unapproved application to market a drug in a different manner, sales and distribution data of a drug manufacturer, profit and loss data, overhead and operating costs, and information on financial condition. For purposes of this exemption, disclosure of the information must either: 1) impair the government's ability to obtain necessary information in the future, or 2) cause substantial harm to the competitive position of the party from whom the information was obtained.	Yes	FOIA Exemption 4 – Proprietary Information Note: The D.C. circuit resolved that the Trade Secrets Act is not considered a statute under Exemption 3 and therefore cannot be cited under FOIA.
Contractor Technical Proposals	Covers contractor technical proposals where the proposal is not set forth or incorporated by reference into an ensuing government contract.	Yes	FOIA Exemption 3: National Defense Authorization Act – 41 U.S.C. Section 253b(m)
Contractor Business Proposals	Covers contractor business proposals.	Yes	FOIA Exemption 4 – Proprietary Information

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Personnel and Human Resources Information			
General Personnel Management	Covers information associated with the recruitment, management, and development of personnel. Such data includes role descriptions, compensation levels, recruiting efforts, the hiring process, benefits management, expense reimbursement, continuing education, career advancement, training and development plans, etc. This category also includes travel management and personnel logistics, except in conjunction with bioterrorism or other homeland security-related events.	No	
Personal Identifying Information and Privacy Act Systems of Records	Covers information identifiable to a specific individual that would constitute a clearly unwarranted invasion of personal privacy – i.e., home address and phone number, social security number, marital status, legitimacy of children, welfare payments, family fights and reputation, medical condition, date of birth, religious affiliation, citizenship data, genealogical history establishing membership in a Native American Tribe, criminal history records (commonly referred to as "rap sheets"), incarceration of United States citizens in foreign prisons, sexual inclinations or associations, and financial status. Note: Personal information that is ***not*** generally protected concerning agency workers include name, title, grade, salary, awards, duty stations, position descriptions, job elements, and performance standards. Note: Foreign nationals are entitled to the same privacy rights under the FOIA as are U.S. citizens.	Yes	FOIA Exemption 6 Also: Privacy Act – Based on the nature and function of the system in question and the scope of the information request. Note: In 1984, Congress explicitly provided that the Privacy Act is not a statute covered under Exemption 3 and therefore cannot be cited under FOIA. Records that do not qualify as exempt under FOIA usually cannot be protected under the Privacy Act.

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Security Clearance and/or Background Investigations	Covers information resulting from background and security investigations.	Yes	FOIA Exemption 6 Also: FOIA Exemption 3: Public Health Security and Bioterrorism Preparedness Act of 2002 – in cases where the investigation is conducted in relation to the possession, handling, or storage of Select Agents and Toxins.
Agency Worker Disclosures	Covers the content of financial disclosures, conflict of interest waivers, and outside activity disclosures sometimes required for Federal employees and contractors. Note: Information concerning high-ranking agency personnel may sometimes still be disclosed.	Yes	FOIA Exemption 3: Ethics in Government Act Note: Consult the agency FOIA Office for information on what is publicly available under the Act.
Misconduct Investigations Concerning Agency Workers	Covers information gathered during investigations of federal employee or contractor misconduct, including the details and results of internal investigations into allegations of impropriety. Note: Information regarding misconduct investigations into the actions of high-ranking federal employees is much more difficult to protect.	Yes	FOIA Exemption 7(A) – while an investigation is pending, must switch to Exemption 6 or other Exemption 7 subparts following closure of the investigation. FOIA Exemption 6 Note: In some instances a ‘glomar’ (neither confirm nor deny) response is appropriate.

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Facilities Management and Physical Protections			
General Facilities and Equipment Management	Covers information regarding the maintenance, administration, and operation of office buildings, laboratories, environmental controls, machinery, and other capital assets considered possessions of the Federal government. Such information includes space management and planning data, diagrams, floor plans, space and equipment management practices, statistics, operational requirements and usage information, maintenance schedules, resource capabilities, etc.	Conditional	
Detailed Facility Plans, Diagrams, and Blueprints	Covers detailed information regarding agency facilities including blueprints, diagrams, containment / storage areas, and schematics as well as laboratory access, contents, and/or construction information that could aid an attacker by facilitating an intrusion or attack.	Yes	FOIA Exemption 2 – Risk of circumvention
Physical Security Protections and Monitoring	Covers information concerning physical controls and procedures where disclosure could facilitate breach and/or compromise of agency facilities or secure areas. Specific examples include: information about alarm systems, codes, locks, keys, electronic key cards, physical entry systems, cameras, guard rotations and standard operating procedures, environmental controls, and identification badges.	Yes	FOIA Exemption 2 – Risk of circumvention
Internal Emergency Response Management	Covers information related to internal emergency response processes, equipment, and capabilities. Includes emergency responder information, response management and evacuation procedures, containment plans, pre-release public relations information, etc.	Yes	FOIA Exemption 2 – Risk of circumvention

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Agency Management Activities			
Strategic and Operational Planning	Covers information involving the activities of determining strategic direction, identifying and establishing programs and processes to enable change, and allocating resources (capital and labor) among those programs and processes. Includes the budgetary formulation; strategic, capital, and resource planning; budget management and improvement processes.	Conditional	
Program Monitoring, Oversight, Audit, and Evaluation	Covers information used to ensure that the operations and programs of the Federal government and its external business partners comply with applicable laws and regulations, and that may be used to prevent waste, fraud, and abuse. Includes information about monitoring, measurement, evaluation, oversight processes, and findings.	Conditional	
Non-Public Agency Plans, Budgets, and/or Policies (In Development and/or Prior to Approval and Release)	Covers agency working documents and supporting research developed during the decision-making process, including items such as pre-release budgets, draft policies, and strategic plans as well as supporting research materials and recommendations from subject-matter experts or other consultants. Note that selected post-decisional materials may be subject to release unless protected under other exemptions.	Yes	FOIA Exemption 5 – Pre-Decisional / Deliberative Also: FOIA Exemption 2 – Risk of circumvention of controls through release of the material (for example – strategic plans for physical or cyber security may qualify). Other exemptions as allowed based on the specific topic under consideration.
Legal Counsel and Affairs	Covers inter- and intra-agency information concerning legal advice, recommendations, opinions, and materials developed under the 'attorney-client' and 'attorney work-product' privileges.	Yes	FOIA Exemption 5

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Agency Operations			
Workplace Policy Management	Covers information related to the development and dissemination of workplace policies such as dress codes, time reporting requirements, telecommuting, etc.	No	
Records Management and Public Relations	Covers agency information related to records management, administrative (non-mission-related) communications, and public relations.	Conditional	
Financial Management	Covers information related to the aggregate set of accounting practices and procedures that allow for the accurate, efficient, transparent, and effective handling of all government revenues, funding, and expenditures. Includes financial reporting, budget management, payment and grant processing, collections and receivables processing, and general accounting management functions	Conditional	
Acquisition and Inventory Control	Covers information associated with purchasing, tracking, and the overall management of goods and services. Includes procurement processes; quality, quantity and location of assets; and the procurement and management of contract services.	Conditional	

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Information Technology			
Communications Infrastructure	Covers information related to agency telecommunications systems, networks, and infrastructures.	Conditional	
General Information Management	Covers information related to the information technology resources and processes required to support or enable mission services. Includes policy and standards development, computing environments, architecture, infrastructure, planning, design, development, change management, maintenance, helpdesk, support, and disposal processes.	Conditional	
Authentication Credentials	Covers authentication information and credentials (specifically user IDs, passwords, pin numbers, and digital certificates). Note that system authentication credentials should be designated with at least the same level of sensitivity concern as assigned to the highest rated (most sensitive) information managed by the system.	Yes	FOIA Exemption 2 – Risk of circumvention
Detailed Computer / Network System Configurations and Management Practices	Covers information regarding the details of agency computer systems such that could be used to facilitate circumvention of acceptable use and protective controls. Specific examples include lists of IP addresses, system architecture diagrams, application source code listing, specification documents, procedural and operational processes, storage locations, disposal practices, etc.	Yes	FOIA Exemption 2 – Risk of circumvention

Information Type	Description and Examples	Potentially Sensitive?	Potential Exemptions
Information Security Protections and Controls	Covers information concerning the security controls, measures, and configuration settings of agency computer systems where disclosure could facilitate circumvention and/or compromise of those systems. Specific examples include: lists of user IDs and passwords, firewall rules, system and network diagrams, specific descriptions of protective controls and/or operational processes (i.e., timing of backups, location of hot site, monitoring practices, etc.), specific identification of sensitive hosts and systems, architecture descriptions, application source code, continuity of operations plan details, and system security plans.	Yes	FOIA Exemption 2 – Risk of circumvention
Vulnerability / Risk Assessments and/or Penetration Test Procedures and Results	Covers information concerning the timing, conduct, participants, processes, tools, results, and derivative reports stemming from vulnerability and risk assessments and/or penetration tests of agency electronic and/or physical systems, facilities, and environments. Includes tests conducted during system Certification and Accreditation (C&A) processes, Office of Inspector General (OIG) audits, annual updates, routine testing and evaluation, and any other assessments as scheduled by agency management.	Yes	FOIA Exemption 2 – Risk of circumvention
Continuity of Operations (COOP) and Disaster Recovery (DR) Plans	Covers COOP and DR plan documents as well as detailed information concerning recovery methods, strategies, tools, providers, agreements, priorities, timeframes, and facilities.	Yes	FOIA Exemption 2 – Risk of circumvention

Exhibit 2: Summary Listing of CDC Common Information Types

Health Information and Mission Support
- Healthcare Information
- Public Health Data and Statistics
- Non-Public Health Data and Statistics (with Personal Identifying Information)
- Mission Support

Incident Investigation and Response
- Public Emergency Response Management
- Investigative Activities
- Strategic National Stockpile

Select Agents and Bioterrorism
- Select Agents
- Bioterrorism Monitoring and Surveillance Activities
- Bioterrorism Events / Suspected Events and/or Response

Third Party Confidential Information
- Third Party Trade Secrets, Confidential, and Proprietary Information
- Contractor Technical Proposals
- Contractor Business Proposals

Personnel and Human Resources Information
- General Personnel Management
- Personal Identifying Information and Privacy Act Systems of Records
- Security Clearance and/or Background Investigations
- Agency Worker Disclosures
- Misconduct Investigations Concerning Agency Workers

Facilities Management and Physical Protections
- General Facilities and Equipment Management
- Detailed Facility Plans, Diagrams, and Blueprints
- Physical Security Protections and Monitoring
- Internal Emergency Response Management

Agency Management Activities
- Strategic and Operational Planning
- Program Monitoring, Oversight, Audit, and Evaluation
- Non-Public Agency Plans, Budgets, and/or Policies (In Development and/or Prior to Approval and Release)
- Legal Counsel and Affairs

Agency Operations
- Workplace Policy Management
- Records Management and Public Relations
- Financial Management
- Acquisition and Inventory Control

Information Technology
- Communications Infrastructure
- General Information Management
- Authentication Credentials
- Detailed Computer / Network System Configurations and Management Practices
- Information Security Protections and Controls

- Vulnerability / Risk Assessments and/or Penetration Test Procedures and Results
- Continuity of Operations and Disaster Recovery Plans

[1] References to CDC also apply to the Agency for Toxic Substances and Disease Registry (ATSDR).