Sandia National Laboratories

Exceptional service in the national interest

Control of Sensitive Information

in a National Security Context

Duane Lindner
Winalee Carter

January 4, 2017

U.S. DEPARTMENT OF ENERGY

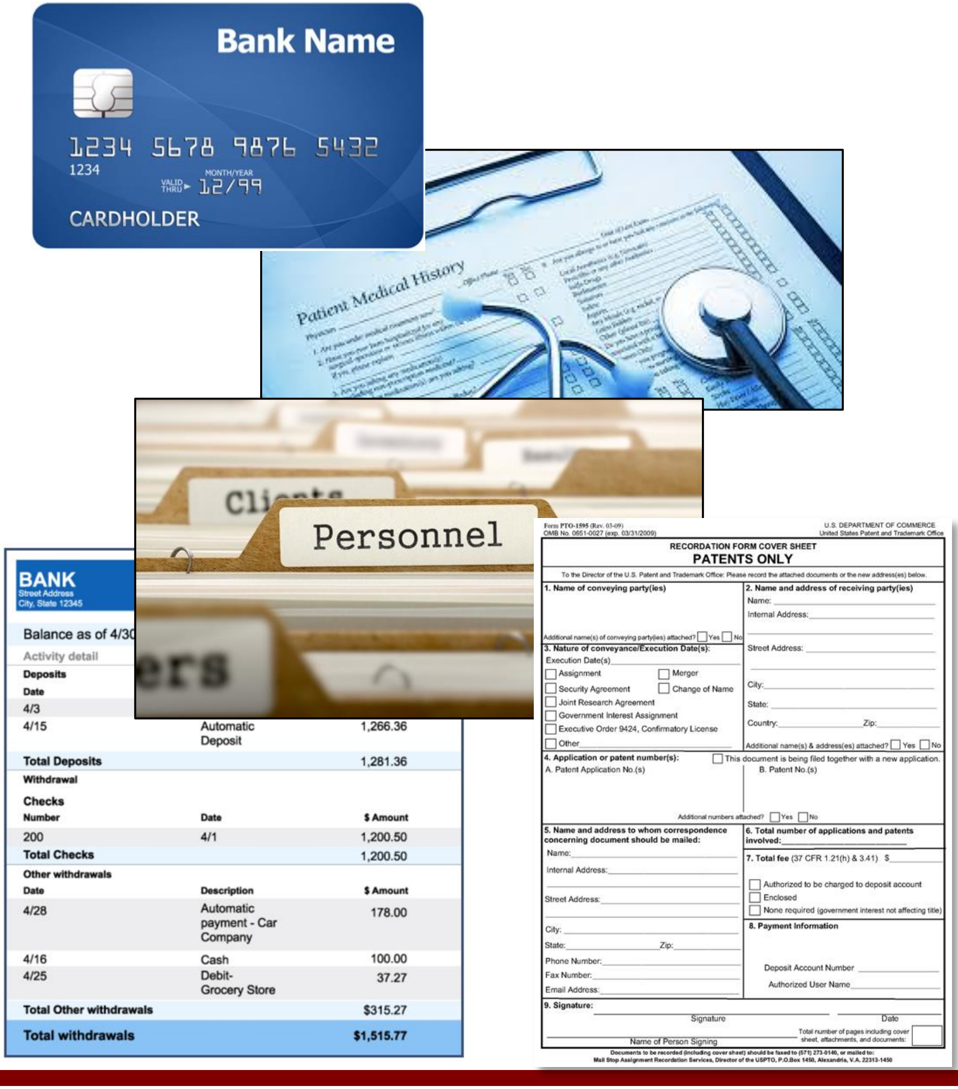
NNSA

SAND2017-0057C

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Management of Sensitive Information

- We are all familiar with control of sensitive information
  - In our personal lives
  - In our workplaces
- Control regimes vary—from “common sense” to legal controls
- Effective management of information is highly dependent on individual action
  - Knowledge of rules and policy
  - Accurate understanding and appreciation of risk
- Management of sensitive national security information relies on the same principles



BANK
Street Address
City, State 12345

Balance as of 4/30

Activity detail

Deposits

Date

4/3

4/15 Automatic Deposit 1,266.36

Total Deposits 1,281.36

Withdrawal

Checks

Number	Date	$ Amount
200	4/1	1,200.50
Total Checks		1,200.50

Other withdrawals

Date	Description	$ Amount
4/28	Automatic payment - Car Company	178.00
4/16	Cash	100.00
4/25	Debit-Grocery Store	37.27
Total Other withdrawals		$315.27
Total withdrawals		$1,515.77

Form PTO-1595 (Rev. 03-09)
OMB No. 0651-0027 (exp. 03/31/2009)

U.S. DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

RECORDATION FORM COVER SHEET
PATENTS ONLY

To the Director of the U.S. Patent and Trademark Office: Please record the attached documents or the new address(es) below.

1. Name of conveying party(ies)

Additional name(s) of conveying party(ies) attached? □ Yes □ No

2. Name and address of receiving party(ies)

Name: ________

Internal Address: ________

Street Address: ________

City: ________

State: ________

Country: ________ Zip: ________

Additional name(s) & address(es) attached? □ Yes □ No

3. Nature of conveyance/Execution Date(s):

Execution Date(s) ________

□ Assignment □ Merger

□ Security Agreement □ Change of Name

□ Joint Research Agreement

□ Government Interest Assignment

□ Executive Order 9424, Confirmatory License

□ Other ________

4. Application or patent number(s): □ This document is being filed together with a new application.

A. Patent Application No.(s)

B. Patent No.(s)

Additional numbers attached? □ Yes □ No

5. Name and address to whom correspondence concerning document should be mailed:

Name: ________

Internal Address: ________

Street Address: ________

City: ________

State: ________ Zip: ________

Phone Number: ________

Fax Number: ________

Email Address: ________

6. Total number of applications and patents involved: ________

7. Total fee (37 CFR 1.21(h) & 3.41) $________

□ Authorized to be charged to deposit account

□ Enclosed

□ None required (government interest not affecting title)

8. Payment Information

Deposit Account Number ________

Authorized User Name ________

9. Signature:

________ Signature ________ Date

________ Name of Person Signing

Total number of pages including cover sheet, attachments, and documents: □

Documents to be recorded (including cover sheet) should be faxed to (571) 273-0140, or mailed to:
Mail Stop Assignment Recordation Services, Director of the USPTO, P.O.Box 1450, Alexandria, V.A. 22313-1450

Classified Information

- Information can be classified under Statute or Executive Order
  - The Atomic Energy Act governs Restricted Data and Formerly Restricted Data
  - EO 13526 governs National Security Information
- Levels of Classification are ”risk based”
  - Confidential: “undue damage to national security”
  - Secret: “serious damage”
  - Top secret: “exceptionally grave damage”
- Management policies are tied to classification category and level

Controlled Unclassified Information (CUI)

68675

Federal Register
Vol. 75, No. 216
Tuesday, November 9, 2010

Presidential Documents

Title 3—

The President

Executive Order 13556 of November 4, 2010

Controlled Unclassified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose.* This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

Sec. 2. *Controlled Unclassified Information (CUI).*

(a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

(c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

Sec. 3. *Review of Current Designations.*

(a) Each agency head shall, within 180 days of the date of this order:

(1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

(b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

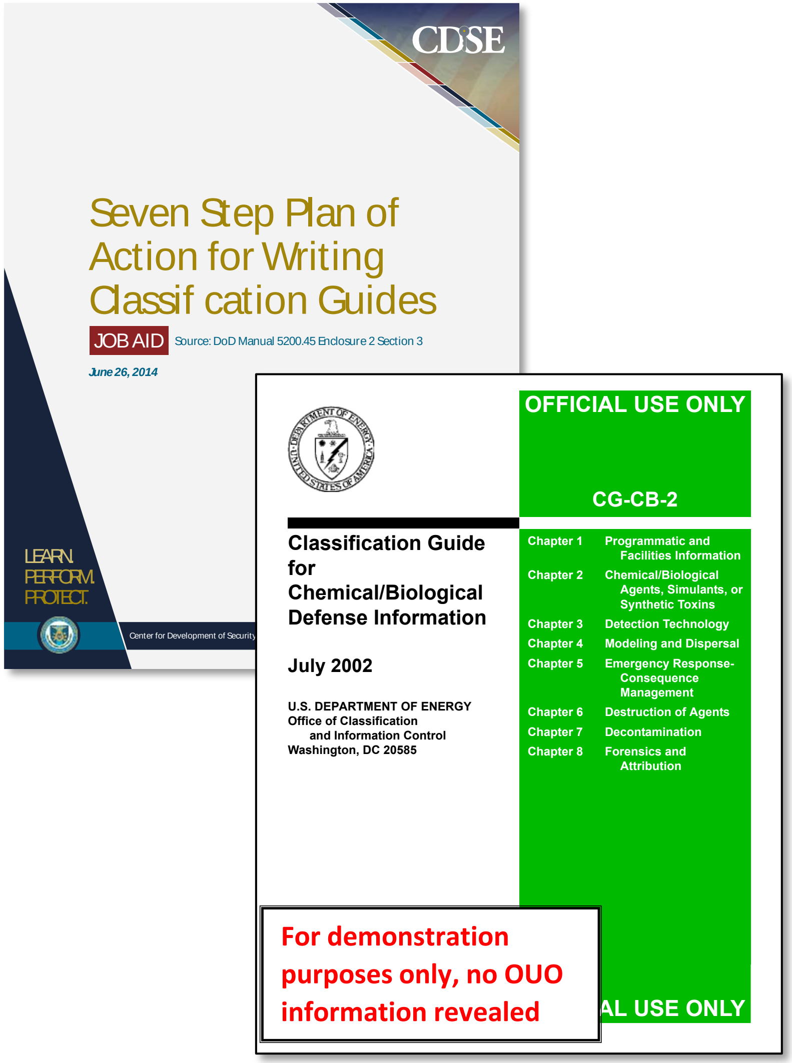
Sec. 4. *Development of CUI Categories and Policies.*

Report and Recommendations
of the Presidential Task Force on
CONTROLLED UNCLASSIFIED INFORMATION

"All unclassified information for which, pursuant to statute, regulation, or agency policy, there is a compelling requirement for safeguarding and/or dissemination controls"

- Subject to EO 13556
- Over one hundred categories are in use across government
- Attempts to regularize categories, policy, access restrictions are ongoing, but having limited success
- Control is much less formal, in most cases
- Management relies on policy, training and adherence to "need to know"

Determination of Information Sensitivity



CDSE

Seven Step Plan of Action for Writing Classif cation Guides

JOB AID Source: DoD Manual 5200.45 Enclosure 2 Section 3

June 26, 2014

LEARN.
PERFORM.
PROTECT.

Center for Development of Security

OFFICIAL USE ONLY

CG-CB-2

Classification Guide for Chemical/Biological Defense Information

July 2002

U.S. DEPARTMENT OF ENERGY
Office of Classification
and Information Control
Washington, DC 20585

Chapter 1	Programmatic and Facilities Information
Chapter 2	Chemical/Biological Agents, Simulants, or Synthetic Toxins
Chapter 3	Detection Technology
Chapter 4	Modeling and Dispersal
Chapter 5	Emergency Response-Consequence Management
Chapter 6	Destruction of Agents
Chapter 7	Decontamination
Chapter 8	Forensics and Attribution

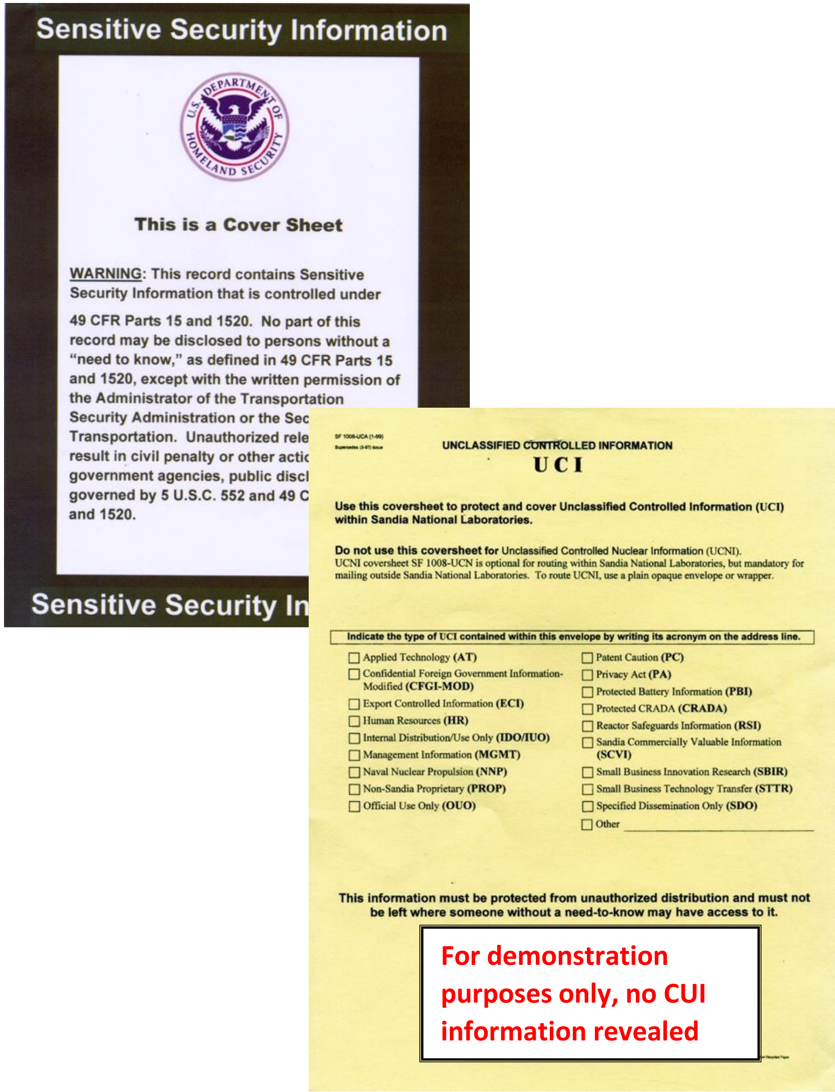
AL USE ONLY

For demonstration purposes only, no OUO information revealed

- Original Classifiers-a few government officials
- Derivative classifiers—many trained individuals
  - Decisions are based on Classification Guides
- Guides are drafted by committees.
  - Some are very information specific
  - Others are broader and "risk informed"
- Approaches for designation CUI are more heterogeneous and less formal
  - CUI frequently governs the "type" of information rather than specific information

Review of documents is a critical procedure to ensure proper classification: to ensure neither underclassification nor overclassification occur.

Control



Sensitive Security Information

This is a Cover Sheet

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Sec
Transportation. Unauthorized rele
result in civil penalty or other actio
government agencies, public discl
governed by 5 U.S.C. 552 and 49 C
and 1520.

Sensitive Security In

SF 1008-UCA (1-99)
Supersedes (3-97) issue

UNCLASSIFIED CONTROLLED INFORMATION

UCI

Use this coversheet to protect and cover Unclassified Controlled Information (UCI) within Sandia National Laboratories.

Do not use this coversheet for Unclassified Controlled Nuclear Information (UCNI).
UCNI coversheet SF 1008-UCN is optional for routing within Sandia National Laboratories, but mandatory for mailing outside Sandia National Laboratories. To route UCNI, use a plain opaque envelope or wrapper.

Indicate the type of UCI contained within this envelope by writing its acronym on the address line.

□ Applied Technology **(AT)**
□ Confidential Foreign Government Information-Modified **(CFGI-MOD)**
□ Export Controlled Information **(ECI)**
□ Human Resources **(HR)**
□ Internal Distribution/Use Only **(IDO/IUO)**
□ Management Information **(MGMT)**
□ Naval Nuclear Propulsion **(NNP)**
□ Non-Sandia Proprietary **(PROP)**
□ Official Use Only **(OUO)**
□ Patent Caution **(PC)**
□ Privacy Act **(PA)**
□ Protected Battery Information **(PBI)**
□ Protected CRADA **(CRADA)**
□ Reactor Safeguards Information **(RSI)**
□ Sandia Commercially Valuable Information **(SCVI)**
□ Small Business Innovation Research **(SBIR)**
□ Small Business Technology Transfer **(STTR)**
□ Specified Dissemination Only **(SDO)**
□ Other ______________________

This information must be protected from unauthorized distribution and must not be left where someone without a need-to-know may have access to it.

For demonstration purposes only, no CUI information revealed

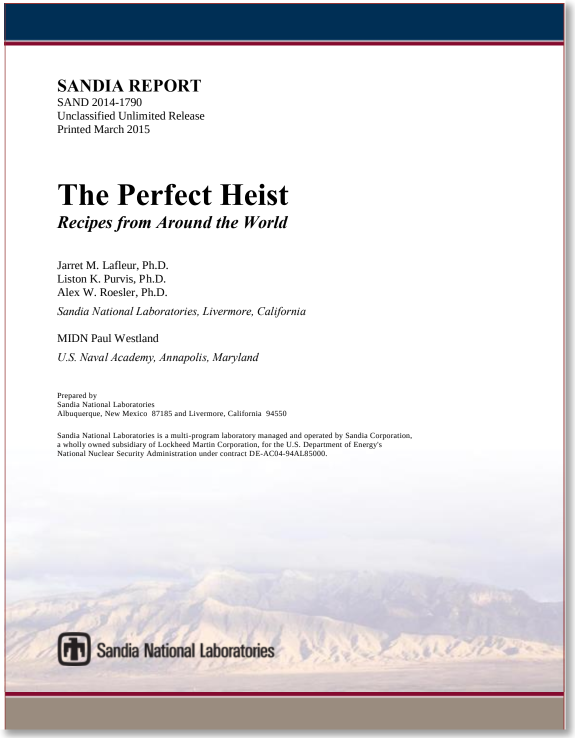
- Policies governing proper identification and control are in place
  - Review at stages
- Sensitive information should be clearly marked
- Sensitive information is stored, handled, and transmitted in specified ways
- Access is limited to authorized individuals with need to know (NTK)
  - Can include clearances, job function, other criteria
- Procedures exist to identify mistakes or accidents
  - Mitigate consequences
  - Inform process improvements

Need to Know (NTK)

The NTK principle is extremely important in managing access to both classified and CUI

- Credentials (clearances or other qualifications) can make a person eligible to access certain information, but such credentials to not establish a right to access information
- NTK management can be very formal
  - With training, formal briefing into (and out of) NTK groups
- In other cases, NTK determination is based on the assessment of individuals who hold information
  - Strong cultural reinforcement enables individuals to deny access to information for which they have no NTK

Environment and Culture



SANDIA REPORT
SAND 2014-1790
Unclassified Unlimited Release
Printed March 2015

The Perfect Heist
Recipes from Around the World

Jarret M. Lafleur, Ph.D.
Liston K. Purvis, Ph.D.
Alex W. Roesler, Ph.D.

Sandia National Laboratories, Livermore, California

MIDN Paul Westland

U.S. Naval Academy, Annapolis, Maryland

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia National Laboratories

- Training is critical
  - At Sandia, training begins (for everyone) upon employment and continues at regular intervals (at least annually)
  - Failure to complete training can (and does) result in automatic loss of access to the workplace
- Awareness
  - Postings, placards, signage throughout the workplace reinforce awareness of sensitive information, risks associated with mishandling it, and individual responsibility
  - Information about adversary attempts to access sensitive information (across government) is regularly shared (as appropriate)
  - Briefings to provide insights into threats to sensitive information can heighten awareness of risk
- Derivative classifiers, management, and information control specialists answer questions and provide both guidance and support

Risk Assessment

- R&D in biology offer enormous benefits to public health and economic prosperity
  - These benefits are widely understood and discussed
- Such work also carries credible risks
  - Risks arise from possible adversary action
  - and from potential accidents
  - While potential risks are discussed, detailed information about them is typically not so available
- In a national security environment, risk information is more widely available
  - Such information is very important in risk/benefit analyses

Control of Sensitive Information Relies on Structure and Culture

- Rules, policies and procedures
  - Guidance
    - Risk informed approaches can be important
  - Training
  - Review of projects, information
    - At all stages
  - Support
- Culture
  - Responsibility
  - Awareness
  - Informed understanding of risk
    - To information
    - To public health