Technical Guidance for Archiving and Configuration Management of Homeland Security Simulation Applications

Charles McLean
National Institute of Standards and Technology
Gaithersburg, MD 20899

Dr. Charles Hutchings
U.S. Department of Homeland Security
Washington, DC 20528

Dr. Sanjay Jain
George Washington University
Washington, DC 20052

Y. Tina Lee
National Institute of Standards and Technology
Gaithersburg, MD 20899

March 2012

U.S. Department of Homeland Security
Washington, DC
and
National Institute of Standards and Technology
Gaithersburg, MD

This page left blank intentionally.

Acknowledgments

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate sponsored the production of this material under Interagency Agreement HSHQDC-09-X-00357 with the National Institute of Standards and Technology (NIST). The work described was funded by the United States Government and is not subject to copyright.

Disclaimers

The findings expressed or implied in this report do not necessarily reflect the official view or policy of the U.S. Department of Homeland Security, U.S. Department of Commerce, or the United States Government.

Some software products may have been identified in context in this report. This does not imply a recommendation or endorsement of the software products by the authors or NIST, nor does it imply that such software products are necessarily the best available for the purpose.

This page left blank intentionally

Executive Summary

This document provides general guidance designed to help the U.S. Department of Homeland Security (DHS) Program Managers and other executives inside and outside of DHS. It is intended to provide useful information that may help personnel better understand the technologies used to maintain and support homeland security modeling and simulation (M&S) applications.

Examples of topics (within the context of simulation) that are addressed in this report include:

- Archiving of simulation applications, associated software, and test data
- Configuration management of simulations, models, associated software, and test data

For each topic, the following information is provided: a brief introduction to the topic, explanation of its significance, definitions of key terminology, and identification of relevant standards. Examples of subtopics include policies and planning, procedures, and tools. Additional information on subtopics will include a discussion of issues, recommendations and guidelines, and sources of further information.

The technical guidance contained in this report is based on published literature, information available on the Internet, technical expertise, and personal experience.

This page left blank intentionally.

Table of Contents

This page left blank intentionally

1 Introduction

Models and simulations can be extremely useful tools for solving difficult problems, understanding the behavior of complex systems, conducting disaster exercises at the local and national levels, and training personnel on organizations, policies, operations, and procedures. The U.S. Department of Homeland Security (DHS) has a broad mission and a wide variety of M&S applications may ultimately be developed to support this mission. For example, M&S applications may be developed to analyze the performance of critical infrastructure systems, train incident management personnel, evaluate resource requirements for healthcare systems, or model the spread of plumes resulting from the release of hazardous materials. Within the context of the DHS M&S applications, development is typically performed by outside contractors, government laboratories, and the academic establishment.

This report provides guidance for personnel involved in the maintenance, support, and deployment of homeland security models and simulations. Personnel may have significant expertise in some areas pertaining to the development of models and simulations, but may be unaware of important issues in other areas due to scope and complexity of M&S within DHS. This document attempts to provide a high-level overview of a number of key areas pertaining to homeland security M&S. It is intended to provide useful information for a range of topics that may help personnel better understand areas that they may not be familiar with, raise key issues, and answer some important questions with respect to those areas.

For the purpose of the scope of this document, M&S applications are limited by information technology and software systems that are primarily used for analysis, management planning, or training needs. Although concepts addressed in this document should be applicable to most DHS M&S domains, it is only intended to focus on four application domains where M&S is currently being applied: critical infrastructure systems, incident management systems, healthcare systems, and hazardous material releases.

1.1 Purpose

This document was prepared to assist personnel who may not be experts in simulation technology, software engineering, and information technology (IT) support functions, to better understand capabilities and issues associated with the maintenance, support, and deployment of M&S applications. Information contained in this report may be useful for the creation of checklists of points to be addressed as new simulation applications are acquired by DHS. The report is intended to help establish a common ground between DHS personnel, external developers, and others in the M&S community. The technical domains covered and topics associated with the development of M&S applications are the subject of a separate report, see [NIST 2011a].

The intended audience for this report are DHS program and project managers, software and IT support personnel including web site administrators, contracting officer’s technical representatives (COTRs), external contractors and researchers, and users of M&S technology within and outside of DHS. The document is being made publicly available through the NIST Publications Portal [NIST 2011b] and is accessible online to all who have interest in this area.

Topics that are the focus of this report are archives and software configuration management of M&S software and data. For each topic, an introduction, key terminology, issues, recommendations and guidance, and pointers to further information are provided.

1.2 Background of M&S Implementation within DHS

Modeling and simulation activities are being actively pursued within DHS and by DHS contractors. DHS M&S activities are constantly evolving. This section introduces some topics pertaining to M&S within DHS, namely: 1) component organizations involved in M&S and 2) roles and responsibilities of DHS staff that potentially have a stake in M&S.

1.2.1 DHS Component Organizations Involved in M&S

DHS is already making widespread use of M&S. This section identifies some of the organizations within DHS that are currently using M&S and how they are using it. M&S capabilities are being used to support a number of different types of risk assessments, analyses, training, exercises, and system engineering needs. Analytical capabilities supporting problem solving and decision making:

- Analysts and analytical expertise
- Analytical methods and processes
- Body of knowledge (data, information, reports, etc.)
- Tools (models, simulations, computational capabilities, experiments, etc.)

For example, the Office of Infrastructure Protection (OIP) Infrastructure Analysis and Strategy Division (IASD) conducts risk analysis supported by contractor analysts and National Laboratory dedicated personnel. IASD manages multiple models/simulations and data sets through a capability portfolio. IASD, in coordination with the Infrastructure Information Collection Division (IICD), acquires a wide variety of both government and commercial data.

A list of M&S capabilities currently used by DHS and an overview of these capabilities are listed in Appendix I. For examples of existing M&S applications for homeland security, please see the report on the DHS-NIST 2011 workshop on Modeling and Simulation Applications for Homeland Security [NIST 2011c].

or examples of existing M&S applications for homeland security, please see the report on the DHS-NIST 2011 workshop on Modeling and Simulation Applications for Homeland Security [NIST 2011c].

1.2.2 DHS Roles and Responsibilities Relevant to M&S

There are a number of positions in different disciplines within DHS that potentially have a stake in the development of homeland security M&S applications. The roles and responsibilities of organization and position types are identified below. [DHS 2011] defines the core team in the DHS Program Management Office (PMO). Identified career fields and related responsibilities include:

- *Program Management:* Acquisition professionals in the program management acquisition discipline are concerned with all of the functions of a PMO. Program management professionals serve in a wide range of PMO and component acquisition staff positions, including program integrators and analysts, program managers, and their deputies. They may also serve in a number of support and management positions throughout the workforce.
- *Systems Engineering*: Systems engineers demonstrate how systems engineering technical and technical management processes apply to acquisition programs; interact with program Integrated Product Teams (IPTs) regarding the proper application of systems engineering processes; develop system models and work breakdown structures; and use top-down design and bottom-up product realization.

- *Acquisition/Financial Management:* Acquisition/Financial Management staff plan, direct, monitor, organize, and control financial resources including: formulation of budget to requirements, execution, financial systems, appropriations-related congressional issues, and reporting. They are responsible for all financial and budgeting for the program.
- *Life Cycle Logistics (LCL) Management:* LCL management is the planning, development, implementation, and management of a comprehensive, affordable, and effective systems support strategy. LCL encompasses the entire system's life cycle including acquisition (design, development, test, produce, and deploy), sustainment (operations and support), and disposal. Life-cycle logisticians perform a principal joint and component logistics role during the acquisition, operational, and disposal phases of the system's life cycle.
- *Test and Evaluation (T&E):* T&E Managers are engineers, scientists, operations research analysts, system analysts, computer scientists, and other technical personnel who plan, perform, and manage T&E tasks in support of all acquisitions. The individuals in T&E positions are subject matter experts who will plan, monitor, manage, and conduct T&E of prototype, new, fielded, or modified IT; non-IT; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR); and infrastructure systems.
- *Cost Analysts*: Cost analysts lead teams in the analysis of schedule requirements, gathering data relevant to the system-to-be cost, development or evaluation of existing cost estimating relationships and mathematical models, performance of risk analysis on program assumptions, analysis of results of models and other methods of developing costs, accumulation of cost estimates made by work breakdown structure elements, and development of summary data for presentation purposes; development in written, graphical and tabular from information on methods and data used during the development of the estimate, reconciliations of program content and methods used by the organization-independent estimate vice those used by the program office of the weapon/information system being costed; preparation of briefings to management in development of cost databases, parametric relationships, cost estimating software and documentation, and research reports.
- *Information Technology (IT)*: IT specialists include computer scientists, information technology management specialists, computer engineers, and telecommunications managers, who directly support the acquisition of information technology. This may include hardware, software, or firmware products used to create, record, produce, store, retrieve, process, transmit, disseminate, present, or display data or information.
- *Contracting Officer's Technical Representative (COTR)*: COTR is a business communications liaison between the United States Government and a private contractor. COTRs ensure that their goals are mutually beneficial. The COTR is responsible for recommending and authorizing (or denying) actions and expenditures for both standard delivery orders and task orders, and those that fall outside of the normal business practices of its supporting contractors and sub-contractors.

This report will focus largely on capabilities, facilities, and services that DHS managers and technical staff will require from IT departments and support personnel in order to establish required archives, perform configuration management functions, and deploy M&S applications.

1.3 Document Overview

Section 2 addresses issues pertaining to the establishment of archives for models, simulations, and test data. Section 3 presents topics relating to software configuration management. Section 4 presents conclusions for this report. Section 5 provides definitions for selected abbreviations and acronyms that appeared in this report. Section 6 identifies references and sources of further information on the topics that were addressed.

2 M&S Archives

Introduction – Retention of M&S software, test data, and associated documentation may not be only useful to future research and development efforts, it may also be legally required as part of the records management regulations for government agencies. Reasons for archiving information may include agency record keeping requirements, items of historical value, and information/evidence that may be required in future legal proceedings (e.g., contractual disputes).

Issues that will need to be addressed with respect to M&S archives include the types of information that will be stored, retention requirements, staff roles and responsibilities, archive locations, storage media, information formats, and indexing requirements.

Examples of M&S information that may be maintained in archives include:

- System or module naming data and conventions
- Brief description of the model
- Contractor/developer identification data
- Key dates of development testing
- Identification of qualified/certified users and/or analysts
- Copies of model code or software used or needed to run the system, e.g., database management software
- Copies of build software used to generate executables
- Source, version data, and where appropriate copies of tools/simulators used to run the model
- System documentation, including explanations on how the system may be modified
- Test case data files and databases
- After Action Reviews, M&S outputs, and other reports
- Traces and logs of test runs
- Verification, Validation, and Accreditation (VV&A) and certification data
- Information on exercises including participants, attendees, press clippings, and photographic images
- Presentations and technical papers associated with M&S applications, analyses, and exercises

As DHS M&S archives grow in size and complexity, it will become more important that key attributes associated with applications are indexed and maintained in databases that facilitate rapid access and retrieval of this information.

The International Organization for Standardization (ISO) has established a standard reference model for archival information systems, i.e., ISO 14721:2003 Space data and information transfer systems – Open archival information system – Reference model. Its purpose is “to establish a system for archiving information, both digitalized and physical, with an organizational scheme composed of people who accept the responsibility to preserve information and make it available to a designated community. This reference model addresses a full range of archival information preservation functions including ingest, archival storage, data management, access, and dissemination. It also addresses the migration of digital information to new media and forms, the data models used to represent the information, the role of software in information preservation, and the exchange of digital information among archives [ISO 2003a].”

NASA prepared the initial draft document to define the ISO Reference Model for an Open Archival Information System (OAIS). The NASA reference model [NASA 2002]:

- provides a framework for the understanding and increased awareness of archival concepts needed for Long Term digital information preservation and access
- provides the concepts needed by non-archival organizations to be effective participants in the preservation process
- provides a framework, including terminology and concepts, for describing and comparing architectures and operations of existing and future archives
- provides a framework for describing and comparing different long term preservation strategies and techniques
- provides a basis for comparing the data models of digital information preserved by archives and for discussing how data models and the underlying information may change over time
- provides a foundation that may be expanded by other efforts to cover long-term preservation of information that is NOT in digital form (e.g., physical media and physical samples)
- expands consensus on the elements and processes for long-term digital information preservation and access, and promotes a larger market which vendors can support
- guides the identification and production of OAIS-related standards

Terminology:

Archive – "a collection of computer files that have been packaged together for backup, to transport to some other location, for saving away from the computer so that more hard disk storage can be made available, or for some other purpose. An archive can include a simple list of files or files organized under a directory or catalog structure (depending on how a particular program supports archiving)." [SearchStorage 2011]

"Also, a long-term storage device, as a disk or magnetic tape, or a computer directory or folder that contains copies of files for backup or future reference.

- a collection of digital data stored in this way.
- a computer file containing one or more compressed files.
- a collection of information permanently stored on the Internet." [DictRef 2011]

Historical materials - includes books, correspondence, documents, papers, pamphlets, works of art, models, pictures, photographs, plats, maps, films, motion pictures, sound recordings, and other objects or materials having historical or commemorative value. [NARA 2011a]

Records management program – "activities, policies, and procedures within an organization to implement the systematic and administrative control of records throughout their life cycle to ensure efficiency and economy in their creation, use, handling, control, maintenance, and disposition." [SAA 2005].

Digital assets management system – "software to support the acquisition, description, tracking, discovery, retrieval, searching, and distribution of collections of digital objects." [SAA 2005]

The subsections that follow provide background discussions, recommendations and guidance, and sources of further information on:

- Data retention policy

- Archival workflow
- Tools

Information sources include published literature, information available from other agencies, and commercial concerns.

2.1 Data Retention Policy

Federal agencies have legal requirements [NARA 2011b] for preserving information that is defined in Records Management by Federal agencies (44 U.S.C. Chapter 31). To the extent that M&S may be used to support policy decisions there may be a need to keep records in this area: "Section 3101 - The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities."

National Archives and Records Administration (NARA) has general responsibilities for records management in the Federal government under 44 U.S.C. Chapter 29 and ultimately is responsible for the permanent preservation of those records that have been identified as having historic value. NARA provides more detailed guidance on agency record keeping requirements in a management guide [NARA 1995]. Topics covered in the guide include:

- Determining record status
- Adequate and proper documentation
- Responsibilities of program managers
- Responsibilities of records managers
- Problem areas in implementing record keeping requirements
- Record keeping requirements checklist
- Using office automation applications: records management guidelines

NARA evaluates technical information as part of the scheduling process to determine if records can be transferred to NARA in accordance with applicable transfer instructions, and to determine if any technical considerations might impede NARA's ability to process and provide future access to the records [NARA 2011c]. The General Accountability Office (GAO) may be involved in determining exceptions to record keeping requirements.

NARA has developed a records management checklist as part of the system-development life-cycle (SDLC) process. It recommends that agencies embed records management requirements in the earliest stages of the SDLC. The checklist identifies where the agency may propose to establish records management review and approval to ensure that sound RM practices are incorporated into the development of its proposed IT systems [NARA 2011d].

Issues – Determining which simulations and data sets may need to be retained is not necessarily a simple and straightforward process. NARA and possibly departmental lawyers should be consulted to determine legal requirements for records retention. Certainly analyses supporting departmental policy or resource allocation decisions would require archiving. Simulations supporting training and exercises of historical significance such as those involving top officials or multiple agencies should also be archived. Multiple copies of runs of routine training simulations that are part of instructional programs may not need to be retained. Models and simulations that may be relevant to legal proceedings will need to be preserved, e.g., contractual disputes or where an injury may have occurred as part of an associated exercise.

Recommendations and Guidance – DHS managers involved in M&S need to establish data retention policies that are minimally based upon legal requirements. Policies should also consider the retention of M&S applications for historical purposes or as background information for future research and development efforts. Naming conventions for digital files should also be included in policy documents.

For Further Information – For policy advice for Federal agencies on the use of PDF formats for storing digital documents, see [NARA 2011c]. [SANS 2002] provides suggestions for establishment of data retention policies, especially for legal purposes. A number of organizations have prepared white papers on suggested file naming conventions, see [Alberta 2005], [NCDCR 2008], and [BNL 2011] for recommendations.

2.2 Archival Workflow Procedures

What is archival workflow? "Archivists typically follow an established workflow in appraising, acquiring, processing, and preserving archival collections, carefully documenting each step along the way and using checklists and other workflow tools to guide the process. As part of their workflow, archives produce a range of documentation, including paper and electronic forms, lists, spreadsheets, databases, catalog records, finding aids in Microsoft Word or EAD, and Web pages." [Spiro 2011]

In [CLIR 2009], the steps of the archival workflow process are defined as follows:

- **Appraisal** – Determining which records should be acquired by the archive and estimating their value as it relates to the goals and mission of the archive.
- **Accession –** Acquiring collections and documenting the transfer of materials through a logbook, database, register, or other means.
- **Arrangement** – Organizing archival collections in accordance with their original order and provenance.
- **Description** – A finding aid that outlines the arrangement of the collection and elucidates its research value. This finding aid enables users to determine what a collection contains, helps archives locate materials, and acts as a record of deposit for donors.
- **Preserve –** Protecting materials from deterioration by re-housing them, removing contaminants, providing treatments, and other means. Preservation is an ongoing process that typically begins soon after the collection is acquired.
- **Provide access –** Enabling people to locate information about the collection through catalog records, finding aids, indexes, and other means.
- **Offer reference services –** Assisting patrons in identifying and using collections. [CLIR 2009]

Indexes will need to be created to maintain a full set of information for each M&S file set to support its future use. This includes descriptive data and version information on the computing platform, special hardware requirements, operating system, simulation environment, database management system, and standard file formats used. Index records will need to support standard naming conventions for attributes on files that are maintained based on operating system and computer platforms, e.g., exe, lib, txt, and doc.

Tables will be needed to identify common naming conventions for general computer files as well as the formats for simulation-environment-specific files.

Issues – Handling the complexity of M&S software applications will require a technical skill set that is beyond that of the typical archivist. Archivists will probably not understand the programs, support software, and data files that are used to run models and simulations. Furthermore, these files will vary depending on the simulation environment involved. Archival efforts will undoubtedly require an M&S analyst and possibly IT support personnel to ensure that archived M&S software and associated information is complete, correct, and re-usable. To ensure quality, software will need to be retrieved from archives and tested to guarantee that the proper items have been included in the archived set of materials.

Also, experts have found that there are significant preservation issues associated with digital media. Long-term storage solutions remain an outstanding issue, i.e., virtually all current media formats, such as CDs and DVDs, tend to fail over time.

Recommendations and Guidance – DHS M&S managers should determine the current state of efforts across the department in the areas of archiving and digital records retention. M&S archival efforts may be able to be "piggy-backed" on current ongoing activities. Appropriate personnel will need to be identified to perform archivist and archivist support functions for M&S software and other digital information. Archival workflow should also be defined in appropriate policy documents. The archival workflow process associated with preserving executable software will require additional steps and checklists beyond those identified above, e.g., the test retrieval, installation or setup, and execution of M&S applications and models.

For Further Information – See [CLIR 2009] for more detailed information on archival workflow processes, documents produced, and additional references. For information on a NIST workshop that addressed issues of long-term knowledge retention see [NIST 2007]. [Digital 2011] defines archival preservation formats and evaluation factors selecting formats for storing digital information.

2.3 Tools

Two different types of tools will be most relevant to the archival process – archive management and file compression software. The first type of software is used to support the archival workflow process. The second type of software is used to place files in convenient, efficient formats for storage and retrieval. Examples of the second type of software include file aggregation tools, such as ZIP file software or PDF file generators, that translate documents into a standard format for commonly available reader software.

Issues – It may take some time to establish retention policies and select tools that will be used on a long-term basis. Interim solutions may be necessary to temporarily manage a growing base of M&S applications and associated digital files.

Recommendations and Guidance – Interim archival management tools should be acquired and implemented by supporting IT personnel to manage emerging M&S collections in the near term. A liaison should be established with the National Archives to determine how to best use their resources in the implementation of long-term data retention solutions.

For Further Information – NARA provides an online toolkit [NARA 2011e] that provides extensive information on resources for managing electronic records. [CLIR 2009] provides criteria for evaluating archival management software as well as a survey of some of the commercially available tools.

3 Software Configuration Management

Introduction – Configuration management (CM) is a set of activities that are designed to: 1) control changes to software systems by identifying software items under CM control, 2) define baseline configurations of sets of items, 3) specify procedures for making changes to those items, 4) define version control mechanisms, 5) control the implementation of changes, 6) audit those changes, and 7) generate reports on the changes that are made. This section presents some of the key components of configuration management: policies and planning, configuration identification, configuration change control, configuration status accounting, and configuration reviews. Configuration management involves identifying the configuration of the M&S applications at given points in time, systematically controlling changes to the configuration, and maintaining the integrity and traceability of the configuration throughout the software lifecycle.

In the realm of homeland security M&S applications, the items that may be placed under configuration management include models, simulations, simulation environments and other support software, test data, and documentation. Other software that is required to create modules and data, diagnose problems, perform maintenance, build run-time systems, update documentation, and/or execute these products may also be placed under CM. Proper CM will help enable the organization to answer the following questions:

- What is the configuration of the M&S application and associated data files?
- What is the process for making changes to the M&S applications?
- Who made a change to the application?
- What changes were made to the application?
- When were the changes made?
- Why were the changes made?
- Who authorized the changes?

Some of the benefits an organization can derive from CM include:

- Increased control over technology assets through improved visibility and tracking
- Enhanced system reliability through more rapid detection and correction of improper configurations that could negatively impact performance
- The ability to define and enforce formal policies and procedures that govern asset identification, status monitoring, and auditing
- Improved asset maintenance through the ability to better utilize proactive, preventative, and predictive measures
- Greater agility through more accurate analysis of the impact of potential changes to hardware, software, firmware, documentation, testing procedures, etc.
- Enhanced reconciliation and management of complex system and infrastructures. [SAManage 2010]

A number of consensus as well as governmental standards for CM have been developed. These standards provide useful information that can be readily applied to CM for homeland security M&S applications. For example, the following consensus standards are currently available:

- ANSI/EIA-649/-1998 American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) National Consensus Standard for Configuration Management addresses CM planning, configuration identification, configuration change management (change control), configuration status accounting, and configuration verification. [GEIA 2011]
- ISO 10007:2003 Quality Management Systems – Guidelines For Configuration Management gives guidance on the use of configuration management within an organization. It is applicable to the support of products from concept to disposal. It first outlines the responsibilities and authorities before describing the configuration management process that includes configuration management planning, configuration identification, change control, configuration status accounting and configuration audit [ISO 2003b].
- IEEE STD/ 828-2005 IEEE Standard for Software Configuration Management Plans – The minimum required contents of a Software Configuration Management (SCM) Plan are established via this standard. This standard applies to the entire life cycle of critical software (e.g., where failure would impact safety or cause large financial or social losses). It also applies to non-critical software and to software already developed. The application of this standard is not restricted to any form, class, or type of software. [IEEE 2005]

Terminology – IEEE STD 610 Standard Glossary of Software Engineering Terminology standardized the definition of the following configuration management terms:

> **Baseline** – (1) a specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. (2) a document or a set of such documents formally designated and fixed at a specific time during the life cycle of a configuration item. (3) any agreement or result designated and fixed at a given time, from which changes require justification and approval.
>
> **Configuration** – (1) the arrangement of a computer system or component as defined by the number, nature, and interconnections of its constituent parts, (2) the functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product.
>
> **Configuration audit** – an audit conducted to verify that the development of a configuration item has been completed satisfactorily, that the item has achieved the performance and characteristics specified in the configuration identification, and that its operational and support documents are complete and satisfactory.
>
> **Configuration control** – the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.
>
> **Configuration control board (CCB)** – group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes.
>
> **Configuration identification** – (1) selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation, (2) the

current approved technical documentation for a configuration item as set forth in specifications, drawings, associated lists, and documents referenced therein.

Configuration index – a CM document that provides an accounting of the configuration items that make up a product.

Configuration item (CI) – an aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the CM process.

Configuration item development record – the development status of a configuration item based on the results of configuration audits and design reviews.

Configuration management (CM) – a discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.

Configuration status accounting – the recording and reporting of information needed to manage a configuration effectively, includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes.

Engineering change – an alteration in the configuration of a configuration item or other designated item after formal establishment of its configuration identification.

Engineering change proposal (ECP) – the documentation by which a proposed engineering change is described and suggested. [IEEE 1990]

Key topics pertaining to the implementation of CM for homeland security M&S applications, data, and documentation are addressed in the following subsections of this document:

- Policies and planning.
- Change management procedures and tools.

For each topic, a brief discussion of issues, recommendations and guidance, and sources of further information are provided. Information sources include published literature, information available from other agencies, and commercial concerns.

3.1 Policies and Planning

What are CM policies and plans? A configuration management policy specifies the procedures by which managed items and systems stored in a configuration management system evolve. Different configuration management systems typically use different policies. Subjects covered in a CM policy may include:

- Applicability – to which organizations and systems does this CM policy apply?
- Required documentation – what types of documentation are required for CM?

- Roles and responsibilities – who is involved in CM and what are their responsibilities?
- Training – what training is available and required for CM?
- Tools – what CM tools are available and in use?
- Methodologies – what CM methodologies are being employed?
- Planning – what plans are required for each system placed under CM?
- System identification – how are systems identified, e.g., naming conventions?
- Tracking and reporting – what types of tracking and reporting mechanisms are used?
- Change control board (CCB) – how is the CCB established, who serves on it, and what are its procedures?

For an example CM policy statement, see [CHHS 2004].

A CM plan for a specific item or system under CM might contain (from EIA STD 649):

Title Page

1. *Purpose of Document*
2. *Scope of Project*
3. *Organization, Roles, and Responsibilities*
4. *Configuration Item Identification*
5. *Change Management*
6. *Configuration Status Accounting*
7. *Configuration Audits*
8. *Applicable Documents*

Issues: Although individual projects within agencies of DHS have implemented configuration management on a case-by-case basis, it does not appear that any general department-wide CM policies or plans currently exist.

Recommendations and Guidance – If a champion does not already exist, DHS should identify one for CM of homeland security M&S. It could then accelerate the development of CM policies and plans for M&S applications by: 1) establishing liaisons other government departments/agencies with strong commitments to CM, 2) studying existing documents from those organizations, and 3) deriving DHS-specific policies and plans from those other agency documents. Some other departments/agencies that appear to have considerable expertise and available information to offer are the Department of Defense (DoD), Department of Transportation (DOT), and the National Aeronautics and Space Administration (NASA). It is recommended that they be starting points for establishing CM liaisons.

For Further Information – The DOT System Engineering Handbook provides extensive information on departmental policies and procedures for configuration management [DOT 2011a]. Pressman provides links to many appropriate references on configuration management [Pressman 2011]. [HUD 2011], [DOT 2011b], [DOT 2011c], and [NIST 2011d] provide templates for configuration management plans.

3.2 Change Management Procedures and Tools

What is change management? It is a process for reviewing, approving, and tracking proposed changes to a system. Costs and benefits of proposed changes are principal criteria for the change review process. The first step of the change process is the completion of a change request form. Change-request forms may typically contain the following types of information:

- Originator: name, phone, organization, and date
- Description of proposed change
- Change justification
- Preliminary assessment
- Urgency
- Impact assessments
- Change control board (CCB) decision

The kinds of issues that the CCB may address include [Toolbox 2011]:

- Schedules
- Interim delivery dates
- Requirements changes
- Design changes
- Source code changes
- Executable code changes
- Library changes
- Documentation changes
- Defects/failures
- Software-related problem resolution

Depending on the size of the organization, the software involved, etc. the CCB may range from a single individual such as a project manager to a group.

Configuration management tools will provide functionality for creating change requests, tracking changes, identifying configuration items, and aggregating among other functions. See [ISO 2010] for a discussion of standard CM tool capabilities.

Issues – Homeland security M&S applications will vary greatly in size, complexity, development costs, number of users, distribution plans, impact of outputs, and decisions resulting from those outputs. As such, CM procedures and tools should be appropriate to the items put under configuration management. It is assumed that perhaps only more significant items by the above criteria may be managed by CM systems. Another issue is that software companies tend to come and go – expected longevity and stability of CM vendors should be an important evaluation criteria.

Recommendations and Guidance – DHS should identify configuration management needs including the number and types of M&S applications that will be placed under configuration management in the foreseeable future. It should perform a survey of available tools and select a tool that comes closest to meeting DHS needs.

For Further Information – For a guide to selection of configuration management tool capabilities, see [ISO 2010]. Concurrent Versions System (CVS) [CVS 2012] is an open source tool that performs some of the functions associated with configuration management. [Eaton 2011] provides a summary of commercially available configuration management tools.

4 Conclusions

This document presented information archiving and configuration management of modeling and simulation (M&S) in a manner and at a level appropriate for DHS Program Managers, project managers, and IT support staff with significant experience and domain knowledge but with limited understanding of the M&S, archiving, or CM technologies. The current status of M&S implementation in DHS was discussed including the relevant policies, DHS component organizations utilizing M&S, and DHS roles and responsibilities relevant to M&S.

This document focused on two key areas of responsibility pertaining to M&S applications that were typically developed and delivered to DHS by outside organizations. Each area was briefly introduced, relevant standards were identified, and terminology was defined. The first area was archiving of digital information, i.e., the establishment of archives for M&S applications and data associated with those applications including technical reports, support software, and information of historical significance. Subtopics included data retention policy, archival workflow, and tools. The second area was configuration management. Configuration management involves the creation of policies, orderly procedures, and documentation to manage changes to M&S applications. Subtopics included policies and planning, change management, and tools.

DHS Program Managers and others inside and outside DHS should find this document a very useful source of overview information on M&S for initiating efforts to archive and manage the configuration of M&S applications. If recommendations are implemented, wide and regular use of this document by the Program Managers should help DHS successfully establish efforts to meet data retention obligations and implement a configuration management program for simulation applications. These efforts should in turn help increase the use of M&S and in the long term, help improve the DHS's performance.

5 Selected Acronyms and Abbreviations

AAR/IP – After Action Report/Improvement Plan
AHRQ – The Agency of Healthcare Research & Quality
AIAA – American Institute of Aeronautics and Astronautics
ALERT – Center of Excellence for Awareness & Location of Explosives-Related Threats
ANSI – American National Standards Institute
API – Application Programmer Interface
ASC – Advanced Simulation and Computing Program
ASME – American Society of Mechanical Engineers
C2I – Center of Excellence in Command, Control and Interoperability
CAMRA – Center for Advancing Microbial Risk Assessment
CCB – Configuration Control Board or Change Control Board
CDC – The Centers for Disease Control and Prevention
CGMOES – Coast Guard Maritime Operational Effectiveness Simulation
CI – Critical Infrastructure Systems
CIKR or CI/KR– Critical Infrastructure and Key Resources
CM – Configuration management
COE – Center of Excellence
COTR – Contracting Officer's Technical Representative
CREATE – Center for Risk and Economic Analysis of Terrorism Events
CTIA – Common Training and Instrumentation Architecture
CVS – Concurrent Versions System
DBMS – Database Management System
DHS – Department of Homeland Security
DMSO – Defense Modeling and Simulation Office
DoD – Department of Defense
DOE – Department of Energy
DOT – Department of Transportation
EOC – Emergency Operations Center
EIA – Electronic Industries Alliance
EPA – Environmental Protection Agency
ESF – Emergency Support Function
EXCIMS – Executive Council for Modeling and Simulation
FAZD – National Center for Foreign Animal and Zoonotic Disease Defense
FDA – Food and Drug Administration
FEMA – Federal Emergency Management Agency
FFRDC – Federally Funded Research and Development Center
GAO – General Accountability Office
GIS – Geographic Information System
GWU – George Washington University
Hazmat – Hazardous Material
HAZUS-MH – Hazards U.S. Multi-Hazard
HHS – Health and Human Services
HITRAC – Homeland Infrastructure Threat and Risk Analysis Center
HSEEP – Homeland Security Exercise and Evaluation Program
HSNRA –Homeland Security Nation Risk Assessment

HSPD – Homeland Security Presidential Directive
HSSAI – Homeland Security Studies and Analysis Institute
HSTA – Homeland Security Threat Assessment
IASD – OIP Infrastructure Analysis and Strategy Division
I&A – Intelligence and Analysis
IC – Incident Command
IEEE – Institute of Electrical and Electronics Engineers
IICD – Infrastructure Information Collection Division
IM – Incident Management
IMAAC – Interagency Modeling and Atmospheric Assessment Center
INS – Incident of National Significance
IPTs – Integrated Product Teams
ISO – International Organization for Standardization
IT – Information Technology
LCL – Life Cycle Logistics
LLNL – Lawrence Livermore National Laboratory
MIPS – Center for Maritime, Island and Port Security
MS or M&S – Modeling and Simulation
MSCO – DoD Modeling and Simulation Coordination Office
MSWG – DoD Modeling and Simulation Working Group
NARA – National Archives and Records Administration
NARAC – National Atmospheric Release Advisory Center
NASA – National Aeronautics and Space Administration
NCBSI – National Center for Border Security and Immigration
NCFPD – National Center for Food Protection and Defense
NDCIEM – Center for Natural Disasters, Coastal Infrastructure, and Emergency Management
NESC – National Exercise Simulation Center
NGB – National Guard Bureau
NGO – Non-Governmental Organization
NIBS – National Institute of Building Sciences
NIMS – National Incident Management System
NIPP – National Infrastructure Protection Plan
NISAC – National Infrastructure Simulation and Analysis Center
NIST – National Institute of Standards and Technology
NNSA – National Nuclear Security Administration
NOAA – National Oceanic and Atmospheric Administration
NPS – National Planning Scenario
NRC – National Research Council
NRF – National Response Framework
NTSCOE – National Transportation Security Center of Excellence
OAD – Operations Analysis Division
OAIS – Open Archival Information System
OIP – Office of Infrastructure Protection
PACER – National Center for the Study of Preparedness and Catastrophic Event Response
PMO – Program Management Office
RAPID – Risk Assessment Process for Informed Decision Making
RDBMS – Relational Data Base Management System
RM – Risk Management
RMA – Office of Risk Management & Analysis

SAA – Society of American Archivists
S&T – DHS Science and Technology Directorate
S/L – State and Local
SCM – Software Configuration Management
SDLC – System Development Life Cycle
SEDI – Homeland Security Systems Engineering and Development Institute
SISO – Simulation Interoperability Standards Organization
SME – Subject Matter Expert
SSP – Stockpile Stewardship Program
START – National Consortium for the Study of Terrorism and Responses to Terrorism
SUMMIT – Standard Unified Modeling Mapping Integration Toolkit
T&E – Test and Evaluation
USNORTHCOM – U.S. Northern Command
USPHS – U.S. Public Health Service
VNN – Virtual News Network
VV&A – Verification, Validation, and Accreditation
WMD - Weapons of Mass Destruction

6 References

[Alberta 2005] “Naming Conventions for Electronic Documents.” Alberta Government. 2005. Available via: https://www.rimp.gov.ab.ca/publications/pdf/DocumentNamingConventions.pdf (Accessed on 30 November 2011.)

[BNL 2011] “File Naming Conventions & Directory Structure.” Brookhaven National Laboratory. Available via: http://www.bnl.gov/webstandards/filenaming.asp (Accessed on 30 November 2011.)

[CHHS 2004] “SID Policy on Configuration Management.” California Health and Human Services Agency Data Center. April 2004. Available via: http://www.bestpractices.osi.ca.gov/sysacq/downloads/osi%20policy%20on%20configuration%20management%20(2458_6).pdf (Accessed on 30 November 2011.)

[CLIR 2009] “Archival Management Software: A Report for the Council on Library and Information Resources.” Council on Library and Information Resources. Washington, DC. 2009. Available via: http://www.clir.org/pubs/reports/spiro/spiro_Jan13.pdf (Accessed on 22 November 2011.)

[CVS 2012] “CVS – Concurrent Versions System v1.12.12:1,”Ximbiot. Available via: http://ximbiot.com/cvs/manual/cvs-1.12.12/cvs_1.html (Accessed on 05 March 2012.)

[DHS 2011] “DHS Acquisition Staffing Survey and Analysis Report, Acquisition Program.” Management Division/Cost Analysis Division, Office of the Under Secretary for Management, U.S. Department of Homeland Security: Washington, DC. May 5, 2011.

[DictRef 2011] “Archive.” Available via: http://dictionary.reference.com/browse/archive (Accessed on 20 November 2011.)

[Digital 2011] “Sustainability of Digital Formats Planning for Library of Congress Collections - Formats, Evaluation Factors, and Relationships.” Available via: http://www.digitalpreservation.gov/formats/intro/format_eval_rel.shtml and http://www.digitalpreservation.gov/formats/intro/intro.shtml (Accessed on 24 November 2011.)

[DoD 2007] “Strategic Vision for DoD Modeling and Simulation.” Office of the Director of Defense Research and Engineering, Washington, DC. August 24, 2007. Available via: http://www.msco.mil/files/Strategic_Vision_Goals.pdf (Accessed on 20 November 2011.)

[DOT 2011a] *“Systems Engineering Guidebook for ITS Web Site.”Department of Transportation.* Federal Highway Administration and the California Department of Transportation. *Available via:* http://www.fhwa.dot.gov/cadiv/segb/ (Accessed on 1 November 2011.)

[DOT 2011b] “Configuration management plan template.” Federal Highway Administration and the California Department of Transportation. Available via: http://www.fhwa.dot.gov/cadiv/segb/views/document/sections/section8/8_4_3.htm (Accessed on 29 November 2011.)

[DOT 2011c] “Configuration Management for Transportation Management Systems Handbook.” Federal Highway Administration and the California Department of Transportation. Available via: http://ops.fhwa.dot.gov/freewaymgmt/publications/cm/handbook/appendixA.htm (Accessed on 29 November 2011.)

[Eaton 2011] “Configuration Management Tools Summary.” Available via: http://www.daveeaton.com/scm/CMTools.html (Accessed on 29 November 2011.)

[EPA 2002] U.S. Environmental Protection Agency, Quality Assurance Project Plans for Modeling, EPA QA/G-5M. Office of Environmental Information, Washington, DC, 2002. Available via: http://www.epa.gov/quality/qs-docs/g5m-final.pdf (Accessed on 05 March 2012.)

[EPA 2009] U.S. Environmental Protection Agency. “Guidance on the Development, Evaluation, and Application of Environmental Models.” EPA/100/K-09/003, Washington, DC. March 2009.

[FEMA 2008] “National Response Framework.” Federal Emergency Management Agency (FEMA) Department of Homeland Security. January 2008. Available via: http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (Accessed on 22 November 2011.)

[GEIA 2011] “ANSI-EIA-649-A-Standard – National Consensus Standard for Configuration Management.” Available from: http://www.geia.org/Standards-And-Publications (Accessed on 20 November 2011.)
Also available from:
http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FEIA-649-A+2004&gclid=CMj-ldDr3KwCFUdn5Qod6GersQ
(Accessed on 20 November 2011.)

[Hollenbach 2009] Hollenbach, J.W. “Inconsistency, Neglect, and Confusion; A Historical Review of DoD Distributed Simulation Architecture Policies” Paper 09S-SIW-077. Simulation Interoperability Workshop (SIW), San Diego, CA. March 23-27, 2009.

[HUD 2011] “Configuration Management Plan.”U.S. Department of Housing and Urban Development. Available via: http://portal.hud.gov/hudportal/documents/huddoc?id=cmptemplate.doc (Accessed on 29 November 2011.)

[Hutchings 2010] Hutchings, C.W. “Improving the Management of Modeling and Simulation Capabilities in the U.S. Department of Homeland Security.” U. S. Department of Homeland Security, Science & Technology Directorate Workshop on Grand Challenges in Modeling, Simulation and Analysis for Homeland Security (MSHAS-2010), Arlington, VA, 17 – 18 March 2010.

[IEEE 1990] IEEE Std 610.12-1990, IEEE standard glossary of software engineering terminology. Institute of Electrical and Electronics Engineers. Available via: http://standards.ieee.org/findstds/standard/610.12-1990.html (Accessed on 18 December 2011.)

[IEEE 2005] IEEE STD 828-2005 - IEEE Standard for Software Configuration Management Plans. Institute of Electrical and Electronics Engineers. Available via: http://standards.ieee.org/findstds/standard/828-2005.html (Accessed on 27 November 2011.)

[ISO 2003a] “ISO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model.” International Organization for Standardization. Available via: http://www.iso.org/iso/catalogue_detail.htm?csnumber=24683 (Accessed on 27 November 2011.)

[ISO 2003b] “ISO 10007:2003 Quality management systems -- Guidelines for configuration management. International Organization for Standardization. Available via: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36644 (Accessed on 27 November 2011.)

[ISO 2010] “ISO/IEC TR 18018:2010 Information technology -- Systems and software engineering -- Guide for configuration management tool capabilities.” International Organization for Standardization. Available via: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51042 (Accessed on 29 November 2011.)

[NARA 1995] “Agency Record keeping Requirements: A Management Guide.” National Archives and Records Administration (NARA). Available via: http://www.archives.gov/records-mgmt/publications/agency-recordkeeping-requirements.html (Accessed on 15 November 2011.)

[NARA 2011a] “National Archives and Records Administration (44 U.S.C. Chapter 21) § 2101. Definitions.” Available via: http://www.archives.gov/about/laws/nara.html#def (Accessed on 22 November 2011.)

[NARA 2011b] “44 USC Chapter 31 - Records Management by Federal Agencies.” Available via: http://www.archives.gov/about/laws/fed-agencies.html (Accessed on 26 November 2011.)

[NARA 2011c] “Tips for Scheduling Potentially Permanent Records in Portable Document

Format (PDF).” National Archives and Records Administration (NARA). Available via: http://www.archives.gov/records-mgmt/publications/pdf-tips.pdf (Accessed on 30 November 2011.)

[NARA 2011d] “Records management toolkit.” National Archives and Records Administration (NARA). November 16, 2011. Available via: http://www.archives.gov/records-mgmt/toolkit/pdf/all-nara-tools-by-date.pdf (Accessed on 30 November 2011.)

[NARA 2011e] “Systems Development Life Cycle Checklists.” National Archives and Records Administration (NARA). Available via: http://www.archives.gov/records-mgmt/initiatives/sdlc-checklist.pdf (Accessed on 30 November 2011.)

[NASA 2002] “Reference Model for an Open Archival Information System (OAIS).” Management Council of the Consultative Committee for Space Data Systems (CCSDS). National Aeronautics and Space Administration. Washington, DC 2002. Available via: http://public.ccsds.org/publications/archive/650x0b1.pdf (Accessed on 15 November 2011.)

[NCDCR 2008] “Best Practices for File-Naming.” North Carolina Department of Cultural Resources. 2008. Available via: http://www.records.ncdcr.gov/erecords/filenaming_20080508_final.pdf (Accessed on 30 November 2011.)

[NIST 2007] Lubell, J., S.Rachuri, E.Subrahmanian, W.Regli. “Long Term Knowledge Retention Workshop Summary - NISTIR 7386.” National Institute of Standards and Technology, Gaithersburg, MD. 2007. Available via: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=822647 (Accessed on 30 November 2011.)

[NIST 2011a] McLean, C., C. Hutchings, Y. T. Lee, S. Jain. Technical Guidance for the Specification and Development of Homeland Security Simulation Applications, National Institute of Standards and Technology: Gaithersburg, MD. November 2011. *(in preparation, for information, contact: [leet@nist.gov].)*

[NIST 2011b] “NIST Publications Portal.” Available via: http://www.nist.gov/publication-portal.cfm (Accessed on 27 November 2011.)

[NIST 2011c] DHS/NIST Workshop on Homeland Security Modeling & Simulation, June 14-15, 2011 (NISTIR 7826). National Institute of Standards and Technology: Gaithersburg, MD. November 2011.

[NIST 2011d] “Configuration Management Plan.” National Institute of Standards and Technology. Gaithersburg, MD. Available via: http://csrc.nist.gov/groups/SMA/fasp/documents/hw_sw_mainenance/Config-Mngment-Plan.doc (Accessed on 27 November 2011.)

[NNSA 2004] National Nuclear Security Administration (NNSA). “ASC Program Plan, FY06, NA-ASC-106R-05-Vol. 1-Rev. 0.” Washington, DC. 2004. https://asc.llnl.gov/publications/asc_program_plan_fy06.pdf (Accessed 05

March 2012.)

[Pressman 2011] “Software Configuration Management.”R.S.Pressman & Associates. Available via: http://www.rspa.com/spi/SCM.html (Accessed on 20 November 2011.)

[SAA 2005] Pearce-Moses, R. “Glossary of archival and records terminology.” Society of American Archivists. 2005. Available via: http://www.archivists.org/glossary/list.asp (Accessed on 15 November 2011.)

[SAManage 2010] “The Benefits of IT Configuration Management.” SAManage. May 14, 2010. Available via: · http://www.samanage.com/blog/2010/05/the-benefits-of-it-configuration-management/ (Accessed on 27 November 2011.)

[SANS 2002] “Electronic Data Retention Policy.” SANS Institute. Available via: http://www.sans.org/reading_room/whitepapers/backup/electronic-data-retention-policy_514 (Accessed on 15 November 2011.)

[SearchStorage 2011] “Definition – Archive.” Available via: http://searchstorage.techtarget.com/definition/archive (Accessed on 20 November 2011.)

[Spiro 2011] Spiro, L. *“Archival Workflow.” Available via:* http://archivalsoftware.pbworks.com/w/page/13600237/Archival%20Workflow (Accessed on 26 November 2011.)

[Toolbox 2011] “SCM: Change Control Board.” Available via: http://it.toolbox.com/blogs/enterprise-solutions/scm-change-control-board-3334 (Accessed on 26 November 2011.)

Appendix I – DHS M&S Capabilities

This appendix presents a list of M&S capabilities currently used by DHS and an overview of these capabilities. Facilities in this appendix may often be sources (i.e., developers) or recipients of M&S homeland security applications. Other likely recipients of deployed homeland security M&S applications include other Federal government agencies, state and local governments, first responder organizations, and various non-governmental organizations (e.g., healthcare institutions, the Red Cross, and faith-based organizations).

Name	Overview
DHS Operations Battle Lab	Mission: To act as the operational DHS and Interagency experimentation and proof of concept center with the express purpose of enhancing and improving current capabilities, situational awareness, and information sharing by leveraging cost effective existing and emerging technologies, concepts, and processes. Goals: • Transform information sharing and reporting by incorporating a single query federated search capability. • Enhance DHS, federal, state and local (S/L), tribal, and private sector access to data, information, and analysis. • Provide DHS, federal, S/L, tribal, and private sector authorities access to an advanced analytical toolkit to support data correlation and fusion. • Enhance interoperability with DoD, U.S. Northern Command (USNORTHCOM), and National Guard Bureau (NGB) during crisis operations. • Enhance situational awareness by integrating interagency, incident command (IC), law enforcement, proprietary, and multiple classification data into a user-defined picture and share via a role and privilege-based interface. • Provide real time data to facilitate timely, risk-mitigated decision making.
Homeland Security Studies and Analysis Institute (HSSAI)	HSSAI is a Federally Funded Research and Development Center (FFRDC) established by the Homeland Security Act of 2002. HSSAI delivers independent and objective analyses and advises in core areas important to all DHS components in support of policy development, decision making, analysis of alternative approaches, and evaluation of new ideas on issues requiring scientific, technical, and analytical expertise. HSSAI efforts are framed around nine strategic capability areas: • Risk analysis – at the strategic, tactical, and operational levels.

	• Operations analysis – to improve real-world processes • Threat analysis – identify and understand existing and emerging threats. • Systems analysis – illuminate complex interdependencies and tradeoffs. • Information-sharing analysis – improve the effectiveness and efficiency of HS operations among all levels of government and the private sector. • Policy and planning analysis – help set the direction for homeland security. • Program analysis – identify solutions for capability gaps. • Science and technology analysis – ensure advances in these areas benefit the end users. • Training, education, and professional development analysis – ensure the necessary competencies for the homeland security workforce.
Homeland Security Systems Engineering and Development Institute (SEDI)	The SEDI FFRDC was established in early 2009 to provide systems engineering expertise and acquisition strategy advice to improve policies, processes, and tools for mission capabilities that ensure the nation's security. SEDI provides an interdisciplinary engineering approach to the challenges of homeland security, combining technical expertise, domain knowledge, and business capabilities to improve interoperability, develop flexible and expandable architectures, and integrate proven technology into practical solutions. Key areas for SEDI work include: • Border security and immigration. • Intelligence and cyber analysis. • Preparedness, response, and recovery. • Protection of critical infrastructure. • Screening and credentialing. • Transportation security.
National Exercise Simulation Center (NESC)	The NESC provides a state-of-the-art facility at FEMA to serve the all-hazards preparedness and response mission through pooling resources, maximizing efficiency, and providing sustained exercise and training support to all stakeholders. NESC will expand its capabilities to: • Support national, federal, state, and local exercises throughout the United States and internationally, with around-the-clock availability, to include Radiological Emergency Preparedness Program exercises and the National Level Exercise with Master Control Cell and National Simulation Cell and related *functions*. • Provide a forum for interagency planners to test their plans (e.g., annual hurricane plans, pandemic influenza plans) by

	providing realistic incident scenarios through which partners can identify gaps and determine courses of action. • Serve as “future planning” support for FEMA's Disaster Operations Directorate and other FEMA and DHS Directorates by providing technical modeling and simulation tools that enable planners to better visualize potential future scenarios. • Coordinate activities that support real-world events and exercises, such as Homeland Security Exercise and Evaluation Program training and initial-, mid-, and final- planning conferences. • Incorporate real-time, mock-media capabilities, such as the Virtual News Network, that provide exercise participants with realistic breaking news bulletins, interviews, and live news coverage of incidents. • Provide practical training opportunities to those learning about exercise design, conduct, and management through individual mentorship of federal, state, tribal, and local professionals. • Link to other centers that provide specialty modeling, simulation and data services such as the Joint War-fighting Center, the National Infrastructure Simulation and Analysis Center, the Emergency Management Institute, and other centers that provide natural and man-made disaster modeling, constructive simulation tools, and Subject Matter Expert (SME) databases and historical deployment/response information. Incorporate national and FEMA improvement management services to include the Remedial Action Management Program, the National Corrective Action Program, and the Lessons Learned Information System, to support in-depth analysis of real-world and exercise events and provide real-time lessons learned capabilities
Office of Infrastructure Protection- Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)/National Infrastructure Simulation and Analysis Center (NISAC)	HITRAC performs threat, vulnerability, and consequence analysis for risk to the National Critical Infrastructure and the capabilities that infrastructure provides. The Modeling, Simulation, and Analysis capability is directed and managed by HITRAC and executed by NISAC. NISAC provides strategic, multi-disciplinary analyses of interdependencies and the consequences of infrastructure disruptions across all 18 critical infrastructure and key resource (CIKR) sectors at National, regional, and local levels. HITRAC manages the capability development and employment of tools for HITRAC and NISAC analysts to address the complexities of interdependent national infrastructures, including process-based systems dynamics models, mathematical network optimization models, physical-science-based models of existing infrastructures, and high-fidelity agent-based simulations of systems.
Office of Intelligence and Analysis (I&A) “Future Series” Workshops	The Strategic Analysis Group has implemented a pilot program of Future Workshops as a follow on the Homeland Security Threat Assessment (HSTA). These workshops have two principal goals. The first is to better integrate intelligence analysts with planning

	and programming analysts across the DHS Enterprise to support capabilities and gaps analysis. The second is to identify Emerging Trends that may impact homeland security, a requirement of the 9/11 Commission emphasis on preventing surprise. The topics of these workshops are derived from the HSTA Threat Streams, but are focused on more detailed levels of analysis of interest to the Policy customer. These workshops have been jointly hosted by the Undersecretary for Intelligence and Analysis and the Undersecretary for Policy.
Office of Risk Management & Analysis (RMA)	RMA was established in April 2007 and delegated its authority (Delegation Number: 17001) to lead DHS's efforts to establish a common framework to address the overall management and analysis of homeland security risk, develop systematic rigorous risk analysis methodologies, and provide core risk-analysis capabilities to be used throughout DHS to enhance homeland security risk management. RMA addresses risks to the Nation from the DHS Enterprise and the broader Homeland Security Enterprise perspectives. RMA leads DHS's efforts to develop a framework and embed a consistent coordinated approach to address the overall management and analysis of homeland security risk. RMA partners with DHS component organizations to develop and apply systematic risk analysis methodologies and to ensure risk information is used effectively to manage homeland security risk. Additionally, RMA is developing and implementing cross-component analysis in the Risk Assessment Process for Informed Decision Making (RAPID) and in the Homeland Security Nation Risk Assessment (HSNRA). The risk information produced through these assessments will inform enterprise level strategic planning and resource allocation processes and decisions.
Science and Technology Directorate (S&T) -- Operations Analysis Division	The Director of the Operations Analysis Division (OAD) is responsible to the S&T Under Secretary as the principal assistant for operations analysis and senior advisor on requirements for operations analysis, initiating and conducting projects as required and overseeing and managing analytical resources within the S&T Directorate. The OAD director is executive agent of the two DHS FFRDCS (HSSAI and SEDI), as well as executive director of the Homeland Security Science and Technology Advisory Committee (HSSTAC). OAD also manages two other programs with cross-Component applicability: • Gaming Simulations conduct seminar games focused on resolving technology transition challenges. These games result in operational capability gap articulation and understanding, as well as identifying potential technology solutions. Games conducted by OAD have helped identify organizational

	impediments to homeland security technology handoff and fielding. Games typically involve participation from multiple DHS Components, private sector, technology experts, and interagency personnel. • Operational Experimentation assists DHS components by conducting experiments in real-world environments that involve actual users and operators (vice scientists and engineers) and a realistic mix of operational systems in addition to those being tested. Operational experiments are focused on the effects of systems on operations, as opposed to test and evaluation, which tends to consider the effects of operations upon systems.
Science and Technology Directorate (S&T) - University Programs Centers of Excellence	The Homeland Security Act of 2002 granted DHS the authority to create university-based Centers of Excellence (COEs). The centers are authorized by Congress and chosen by the S&T through a competitive selection process. "The Secretary, acting through the Under Secretary for Science and Technology, shall designate a university-based center or several university-based centers for homeland security. The purpose of the center or these centers shall be to establish a coordinated, university-based system to enhance the Nation's homeland security." – as amended. The COEs bring together leading experts and researchers to conduct multidisciplinary research and education for homeland security solutions. Each center is led by a university in collaboration with partners from other institutions, agencies, laboratories, think tanks, and the private sector. Current COEs include: • The Center for Risk and Economic Analysis of Terrorism Events (CREATE), led by the University of Southern California, develops advanced tools to evaluate the risks, costs and consequences of terrorism, and guides economically viable investments in countermeasures that will make our Nation safer and more secure. • The National Center for Foreign Animal and Zoonotic Disease Defense (FAZD), led by Texas A&M University, protects against the introduction of high-consequence foreign animal and zoonotic diseases into the United States, with an emphasis on prevention, surveillance, intervention, and recovery. • The National Center for Food Protection and Defense (NCFPD), led by the University of Minnesota, defends the safety and security of the food system from pre-farm inputs through consumption by establishing best practices, developing new tools, and attracting new researchers to

	prevent, manage, and respond to food contamination events • The National Consortium for the Study of Terrorism and Responses to Terrorism (START), led by the University of Maryland, makes decisions on how to disrupt terrorists and terrorist groups, while strengthening the resilience of U.S. citizens to terrorist attacks. • The Center for Advancing Microbial Risk Assessment (CAMRA), led by Michigan State University, Drexel University, and established jointly with the U.S. Environmental Protection Agency, fills critical gaps in risk assessments for decontaminating microbiological threats, such as plague and anthrax, and answering the question, “How Clean is Safe?” • The National Center for the Study of Preparedness and Catastrophic Event Response (PACER) led by Johns Hopkins University, optimizes our nation's preparedness in the event of a high-consequence natural or man-made disaster, as well as develops guidelines to best alleviate the effects of such an event. • The Center of Excellence for Awareness & Location of Explosives-Related Threats (ALERT), led by Northeastern University in Boston, MA and the University of Rhode Island in Kingston will develop new means and methods to protect the nation from explosives-related threats, focusing on detecting leave-behind Improvised Explosive Devices, enhancing aviation cargo security, providing next-generation baggage screening, detecting liquid explosives, and enhancing suspicious passenger identification. • The National Center for Border Security and Immigration (NCBSI), led by the University of Arizona in Tucson (research co-lead) and the University of Texas at El Paso (education co-lead), is developing technologies, tools, and advanced methods to balance immigration and commerce with effective border security, as well as assess threats and vulnerabilities, improve surveillance and screening, analyze immigration trends, and enhance policy and law enforcement efforts. • The Center for Maritime, Island and Port Security (MIPS), led by the University of Hawaii in Honolulu for maritime and island security and Stevens Institute of Technology in Hoboken, New Jersey, for port security, will strengthen maritime domain awareness and safeguard populations and properties unique to U.S. islands, ports, and remote and extreme environments. • The Center for Natural Disasters, Coastal Infrastructure, and Emergency Management (NDCIEM), led by the University of North Carolina at Chapel Hill and Jackson State University in Jackson, Mississippi will enhance the Nation's

	ability to safeguard populations, properties, and economies as it relates to the consequences of catastrophic natural disasters. • The National Transportation Security Center of Excellence (NTSCOE), was established in accordance with HR1, Implementing the Recommendations of the 9/11 Commission Act of 2007, in August 2007. NTSCOE is made up of seven institutions: Connecticut Transportation Institute at the University of Connecticut, Tougaloo College, Texas Southern University, National Transit Institute at Rutgers - The State University of New Jersey, Homeland Security Management Institute at Long Island University, Mack Blackwell National Rural Transportation Study Center at the University of Arkansas, and the Mineta Transportation Institute at San José State University. The NTSCOE will develop new technologies, tools and advanced methods. The goal is to defend, protect, and increase the resilience of the nation's multi-modal transportation infrastructure and education and training baselines for transportation security geared towards transit employees and professionals. • The Center of Excellence in Command, Control and Interoperability (C2I), led by Purdue University (visualization sciences co-lead) and Rutgers University (data sciences co-lead), will create the scientific basis and enduring technologies needed to analyze massive amounts of information from multiple sources to more reliably detect threats to the security of the nation and its infrastructures, and to the health and welfare of its populace. These new technologies will also improve the dissemination of both information and related technologies.