INSTITUTE FOR DEFENSE ANALYSES

Hardware Assurance Interactions with DMSMS and Parts Management: Is it Oil and Water? Or Oil and Vinegar?

Jay Mandelbaum
Christina M. Patterson

February 2022
Approved for public release;
distribution is unlimited.
IDA Document NS D-32930
Log: H 21-000498

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22301

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0045-14-D-0001, project DE-6-3405, “Fostering Proactive Diminishing Manufacturing Sources and Material Shortages (DMSMS) and Parts Management,” for the Defense Standardization Program Office (DSPO) through the Defense Logistics Agency (DLA). The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information:
Dr. Jay Mandelbaum, Project Leader
jmandelb@ida.org, 703-845-2123
ADM John C. Harvey, Jr., USN (ret) Director, SFRD
jharvey@ida.org, 703-575-4530

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-32930

Hardware Assurance Interactions with DMSMS and Parts Management: Is it Oil and Water? Or Oil and Vinegar?

Jay Mandelbaum
Christina M. Patterson

This page is intentionally blank.

Executive Summary

Diminishing manufacturing sources and material shortages (DMSMS) management is a multidisciplinary process to identify risks resulting from obsolescence, loss of manufacturing sources, or material shortages; to assess the potential for negative impacts on schedule or readiness; to analyze potential mitigations; and then to implement the most cost-effective resolution. Parts management is an engineering discipline for selecting parts for use in a Department of Defense system (or equipment) and take into account considerations that affect the design, production, operation, support, and disposal throughout the life cycle of the system. In March 2022, a Parts and Material Management Conference (PMMC) will cover both topics. The Institute for Defense Analyses (IDA) prepared or substantially helped craft seven briefings for this event.

Three of the briefings will be used for training; they will be presented by DOD practitioners.

- Standardization-related Document (SD) 22 is DOD's overarching DMSMS guidance. DOD published an updated SD-22 (written by IDA) in January 2021 and IDA is preparing another update. NS D-32993 is a substantially modified three-hour training course on the SD-22 processes.
- Development of a DMSMS Management Plan (DMP) is an important early step in DMSMS management. The January 2021 and forthcoming SD-22s formalized DMP development guidance. NS D-32973 is new DMP preparation training.
- •DOD prime contractors perform many DMSMS procedures and even more parts management procedures. NS D-32996 makes minor revisions to existing training on DMSMS contracting and adds preliminary parts management contracting material.

IDA will present the remaining four briefings in technical sessions. These briefings cover the results of specific subtasks from several IDA projects performed in the last two years.

- NS D-32929 provides a detailed explanation of often-misunderstood DMSMS management interfaces with product, product improvement, supportability, and technology roadmaps. This material is a large part of the forthcoming SD-22 revision.

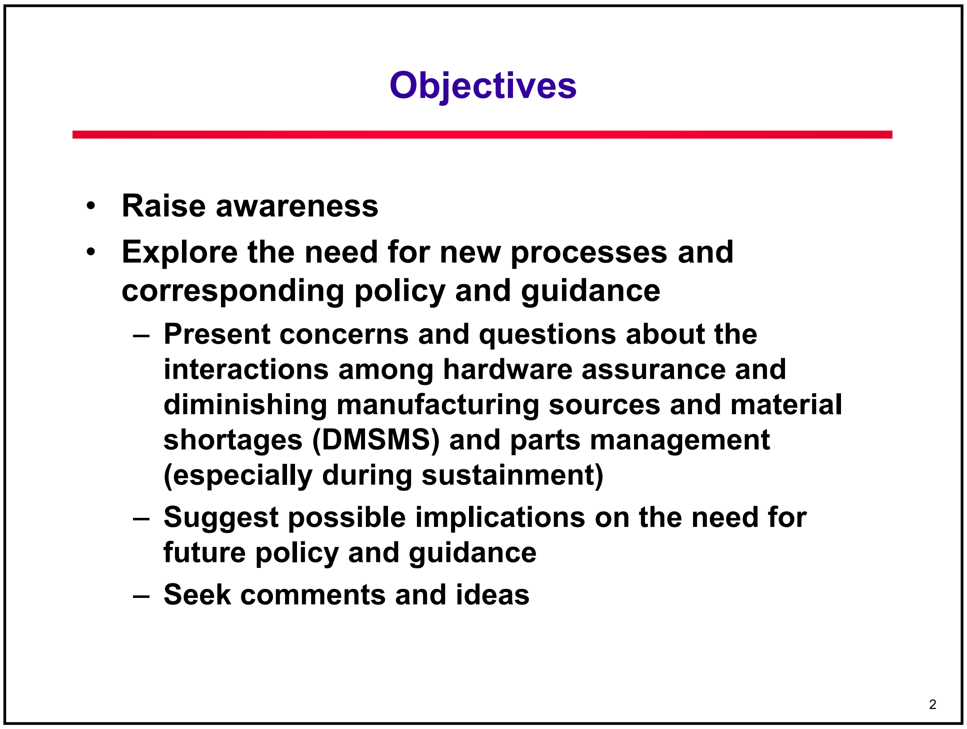
- NS D-32956 describes how to improve the content of manufacturing readiness assessments (MRAs) through a more rigorous consideration of DMSMS management and parts management in the assessment criteria. MRAs are regulatory requirements throughout DOD's acquisition process.
- •NS D-32930 delves into cybersecurity and hardware assurance (HwA) considerations associated with implementing resolutions to DMSMS issues. IDA will also moderate a plenary panel on this subject at the PMMC. IDA plans to use these events to help formulate future policy recommendations.
- NS D-32962 defines new DMSMS resolutions and estimates their average cost. These changes contribute to a more accurate estimate of cost avoidance from proactive DMSMS management and also provide program offices with an initial estimate of resolution cost when no other information is readily available.

Hardware Assurance Interactions with DMSMS and Parts Management: Is it Oil and Water or Oil and Vinegar?

Presented to the
Parts and Material Management Annual Conference
March 7 – 10, 2022

IDA

Jay Mandelbaum
Christina M. Patterson
Institute for Defense Analyses



Objectives

- Raise awareness
- Explore the need for new processes and corresponding policy and guidance
  - Present concerns and questions about the interactions among hardware assurance and diminishing manufacturing sources and material shortages (DMSMS) and parts management (especially during sustainment)
  - Suggest possible implications on the need for future policy and guidance
  - Seek comments and ideas

Outline

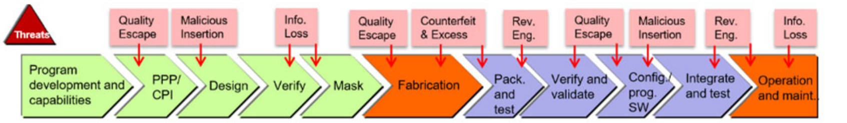
- Introduction
  - Hardware assurance importance
  - Relationship to DMSMS and parts management
- The current situation
  - What needs to be done to take hardware assurance into account
  - As is situation
  - Potential gaps
- Questions about need for new policy and guidance

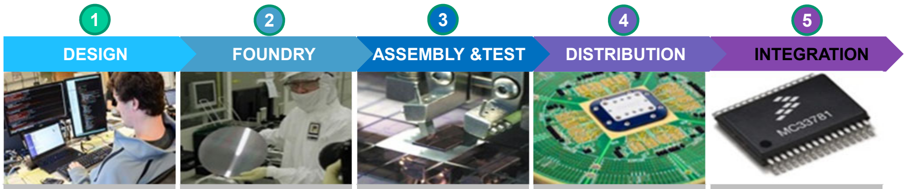
What is Hardware Assurance (HwA)?

- The processes, practices, or methodologies employed to achieve a level of confidence that microelectronics function as intended and are free of exploitable weaknesses and known vulnerabilities, either intentionally or unintentionally designed or inserted, throughout the life cycle
- Note: Microelectronics (also known as microcircuits, semiconductors, and integrated circuits) include the material physical components, programmable logic devices, and interfaces with embedded software and/or intellectual property

Source SAE draft JA7496 Cyber Physical System Security Engineering Plan.
Note that DAU definition is not the same. One key difference is the use of the word "exploitable."

Why is HwA Important?





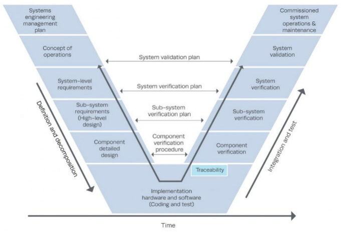
DESIGN	FOUNDRY	ASSEMBLY &TEST	DISTRIBUTION	INTEGRATION
• IP theft / 3PIP • Malware insertion • Design related weaknesses & vulnerabilities	• IP theft • Overproduction • Malware insertion • Reverse engineering	• Malware insertion • Reverse engineering • Sabotage	• Reverse engineering • Malware activation • Bad parts sent to Gray Market	• Operational vulnerabilities • Operational data exposure & theft

The threat landscape is enormous. An independent group of subject matter experts disseminates dozens of pages of security alerts weekly

Sources: Warren Savage, Institute for Systems Research, University of Maryland/Jeremy Muldavin, DASD/DOD, Don Davidson, Synopsys, Inc.

When Should HwA be Considered?

- As part of the systems engineering process to design and develop a product or system
- Whenever a triggering event occurs
  - – An occurrence such as*
    - Changes in the existing design or interfaces
    - Changes in the risk profile of the system and its external supporting processes or procedures
    - Planned assessments of software and systems security engineering concerns
  - – A triggering event should result in a new risk assessment and a reengagement of the systems engineering process if warranted to address the risk


Systems engineering management plan
Concept of operations
System-level requirements
Sub-system requirements (High-level design)
Component detailed design
Implementation hardware and software (Coding and test)
Component verification
Sub-system verification
System verification
System validation
Commissioned system operations & maintenance
System validation plan
System verification plan
Sub-system verification plan
Component verification procedure
Traceability
Definition and decomposition
Integration and test
Time

* SAE draft JA7496 Cyber Physical System Security Engineering Plan

Why Should we be Concerned About HwA?

- The DMSMS management community recommends resolutions to DMSMS issues
  - Nearly every resolution involves changes to the parts on the system or their sources
  - Appropriate protections must be incorporated into the resolution
- Once resolution implementation begins, the parts management community selects new parts and determines the extent of reuse and/or resourcing of existing parts
  - New parts must be free of vulnerabilities and weaknesses that cannot be mitigated to an acceptable level of risk
  - Even existing parts could be a risk since vulnerabilities and weaknesses may have been discovered since initial usage

Part selection and implementation of DMSMS resolutions are triggering events, risk can increase significantly

Outline

- Introduction
  - Hardware assurance importance
  - Relationship to DMSMS and parts management
- The current situation
  - What needs to be done to take hardware assurance into account
  - As is situation
  - Potential gaps
- Questions about need for new policy and guidance

Logical Steps for Taking HwA into Account

1. Determine DMSMS cases where HwA should be a consideration
   - Include HwA in scoping resolution options where appropriate
2. Avoid selecting parts with known vulnerabilities or exploitable weaknesses when developing resolutions, if possible, otherwise mitigate risks
   - Supply chain threats should be considered when pedigree and traceability are unknown or parts are acquired from an untrusted source (e.g. brokers or untrusted fabs)
3. Incorporate (1) and (2) when implementing resolutions

Next we will
- Explore some basic elements of each of these steps
- Make initial observations on an "as is" situation and potential gaps

Where Should HwA be a Consideration? (1 of 3)

- Program protection plan (PPP)
  - The purpose of the PPP is to help programs ensure that they adequately protect capabilities, technology, components, and information
  - The process of preparing a PPP involves thinking through what needs to be protected (on the system, its training equipment, or its support equipment) and developing a plan to provide the appropriate protection
  - A PPP is based on an initial criticality analysis and a threat analysis to determine candidate Critical Program Information (CPI)
  - Potential countermeasures and the Acquisition Cybersecurity Strategy are part of the PPP

CPI identification implies that a list of the parts, assemblies, and software that need protection can be generated

Where Should HwA be a Consideration? (2 of 3)

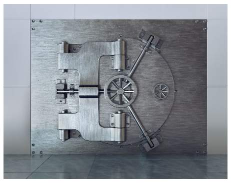
- HwA should be a consideration on any DMSMS case associated with an item that needs protection based on its relationship to CPI
- The DMSMS community should have access to the CPI and therefore is in a position to make such a determination

Where Should HwA be a Consideration? (3 of 3)

- Observations
  - Some program offices (especially those early in the life cycle) do a good job (or are planning to do a good job)
    - Cannot say anything about how that may change over the life cycle
  - Some program offices actively seek exemptions from preparing a PPP; legacy programs may not have PPPs
  - PPPs may be out of date
  - Some programs do not prioritize funding to update the PPP
  - Some DMSMS practitioners have no interface with the PPPs
  - Some program offices do not have sufficient or timely information about the threats

There is a strong potential for gaps—HwA cannot be a consideration if the information is not used or available

How can Parts with Vulnerabilities or Weaknesses be Avoided or Otherwise Mitigated? (1 of 3)



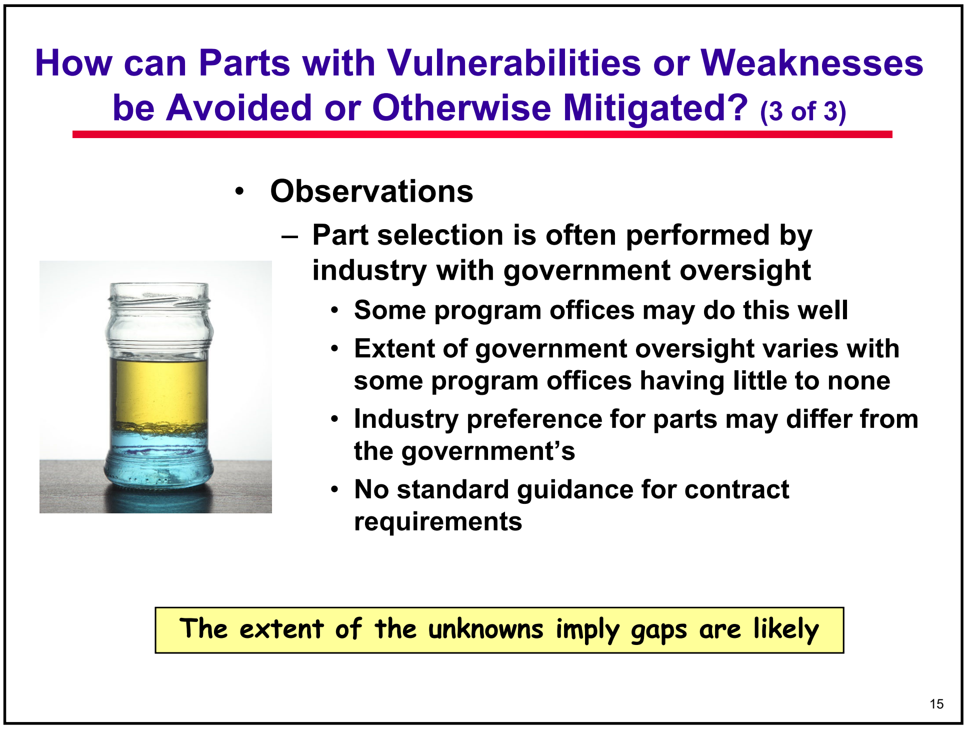
- MITRE publishes Common Vulnerability Enumeration (CVE), Common Weakness Enumeration (CWE), and Common Attack Pattern Enumeration and Classification (CAPEC) lists
  - CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts
  - The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities
  - CAPEC™ is a comprehensive dictionary and classification taxonomy of known attacks that can be used to enhance defenses

These lists imply parts that require mitigation or avoided altogether where possible

How can Parts with Vulnerabilities or Weaknesses be Avoided or Otherwise Mitigated? (2 of 3)

- Program offices themselves as well as their prime contractors could build criteria into their parts selection process for risks
  - CVEs and CWEs
  - Opportunities to compromise parts address parts management requirements in other domains of considerations
    - Electronic security
    - Physical security
    - Information protection
    - Data & information security
    - Asset management
    - Access control
    - Life cycle support
    - Obsolete
    - Anti-counterfeit
    - Cyber-SCRM
    - Application security
    - Issues and events management
    - Traceability and tracking
    - Anti-malicious
    - Anti-tamper
    - Information sharing & reporting

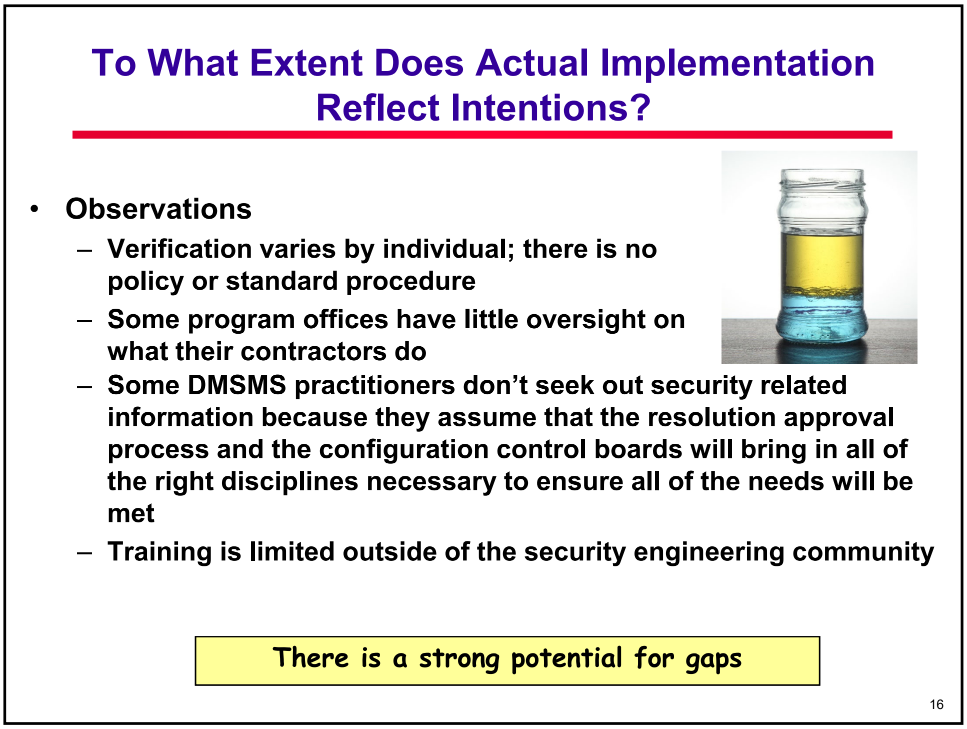
Avoid selecting parts with known vulnerabilities or exploitable weaknesses if possible. Otherwise alert security engineering to mitigate risks (which are likely to impact prior part selections)



How can Parts with Vulnerabilities or Weaknesses be Avoided or Otherwise Mitigated? (3 of 3)

- Observations
  - Part selection is often performed by industry with government oversight
    - Some program offices may do this well
    - Extent of government oversight varies with some program offices having little to none
    - Industry preference for parts may differ from the government's
    - No standard guidance for contract requirements

The extent of the unknowns imply gaps are likely



To What Extent Does Actual Implementation Reflect Intentions?

- Observations
  - Verification varies by individual; there is no policy or standard procedure
  - Some program offices have little oversight on what their contractors do
  - Some DMSMS practitioners don't seek out security related information because they assume that the resolution approval process and the configuration control boards will bring in all of the right disciplines necessary to ensure all of the needs will be met
  - Training is limited outside of the security engineering community

There is a strong potential for gaps

Outline

- Introduction
  - Hardware assurance importance
  - Relationship to DMSMS and parts management
- The current situation
  - What needs to be done to take hardware assurance into account
  - As is situation
  - Potential gaps
- Questions about need for new policy and guidance

Where Should HwA be a Consideration?

- Questions on closing the gaps
  - Is the PPP the most appropriate starting point?
  - Are there ways to supplement?
  - Other sources of parts posing significant risks?

How can Program Offices Avoid Selecting Parts with Vulnerabilities or Weaknesses? (3 of 3)

- Questions on closing the gaps
  - Should there be interfaces with Cyber Command (CYBERCOM)?
    - Is it just software?
  - Should there be interfaces with the Cybersecurity and Infrastructure Security Agency (CISA)?
  - Should there be interfaces with the Joint Federated Assurance Center (JFAC)?
  - Should there be interfaces with CAPEC?
  - Is there a classified version of CVE/CWE?
  - Anything else?

To What Extent Does Actual Implementation Reflect Intentions?

- Questions on closing the gaps
  - There is an SD-22 best practice that the DMSMS community should remain aware of implementation actions (at a minimum) and possibly monitor the stakeholders to ensure they are meeting their responsibilities
    - Does that need greater emphasis?
    - What about when the contractor does the work, should there be additional contractor reporting requirements?

Broad Policy and Guidance Questions

- Should there be parts management policy on when and where to require government approval of parts?
  - Just for CPI associated parts?
  - What about
    - Critical safety?
    - Nuclear propulsion?
    - Emerging technology elements (ETE)?
    - Anything else?

- To what extent does DMSMS policy and guidance need to change to minimize the likelihood of an HwA issue being missed?
  - Greater emphasis on interfaces with security engineering in guidance?
  - Does DoDI 4245.15 need to change?
- Who are the other players? What is their role?

Even Broader Policy and Guidance Questions

- What about depot maintenance during sustainment where DMSMS resolutions may be implemented and parts may be selected?
  - Currently no policy or guidance
- What about the value of commercial standards?
  - On what subjects?
  - How might that help close the gaps?
- Is centralized parts management policy valuable or are diverse policies sufficient?
  - Should there be policy on metrics and reporting?
  - Should there be policy on when to use trusted sources or related concepts?
  - Should there be policy on other MIL STD 3018 or MIL STD 11991 requirements?

This page is intentionally blank.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE (DD-MM-YY) XX-02-2022	2. REPORT TYPE Final	3. DATES COVERED (From – To)

4. TITLE AND SUBTITLE

Hardware Assurance Interactions with DMSMS and Parts Management: Is it Oil and Water? Or Oil and Vinegar?

5a. CONTRACT NO.

HQ0034-14-D-0001

5b. GRANT NO.

5c. PROGRAM ELEMENT NO(S).

6. AUTHOR(S)

Jay Mandelbaum
Christina M. Patterson

5d. PROJECT NO.

5e. TASK NO.

DE-6-3405

5f. WORK UNIT NO.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
730 East Glebe Road
Alexandria, Virginia 22301

8. PERFORMING ORGANIZATION REPORT NO.

IDA Document NS D-32930
IDA Log H 21-000498

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

DLA
Defense Standardization Program Office
Suite 1742, Cubicle 17L-H2
8725 John J Kingman Rd, Stop 5100
Fort Belvoir, VA 22060-6220

10. SPONSOR'S / MONITOR'S ACRONYM(S)

DLA-DSPO

11. SPONSOR'S / MONITOR'S REPORT NO(S).

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Hardware assurance (HwA) encompasses the processes, practices or methodologies employed to achieve a level of confidence that microelectronics function as intended and are free of exploitable weaknesses and known vulnerabilities, either intentionally or unintentionally designed or inserted, throughout the life cycle. To achieve an acceptable level of risk, HwA must be addressed in areas such as physical security, electronic security, supply chain risk management, anti-counterfeit, anti-tamper, etc. Resolutions to DMSMS issues nearly always result in part changes and consequently could introduce HwA risks, because—

• The need for protection may not have been communicated to the DMSMS management community
• Existing protections may not be effective for the new resolution or may be out-of-date
• Risks may have changed
• Weaknesses and vulnerabilities may have changed

This briefing will recount experiences garnered from discussions with multiple program offices to capture how HwA is being taken into account when resolving DMSMS issues. Tentative conclusions will be drawn about the seriousness of the problem and the need to take action. Finally, hypotheses concerning approaches to address the risks will be suggested.

15. SUBJECT TERMS

DMSMS management

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NO. OF PAGES	19a. NAME OF RESPONSIBLE PERSON Robin Brown
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include Area Code)
U	U	U	U	20	(571) 363-8630

This page is intentionally blank.