Joint Product Manager

Biological Detection Systems

JOINT
PRODUCT MANAGER
BIOLOGICAL
DETECTION
SYSTEMS

ONE Team Committed to Integrity, Quality and Action

Operations Security (OPSEC) Plan

14 April 2006

DISTRIBUTION STATEMENT D – Further dissemination only as directed by Joint Product Office Biological Detection Systems or higher DoD authority.

WARNING – This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751 et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., app 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

DESTRUCTION NOTICE – For classified documents, follow the procedures in DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), Chapter 5, Section 7, or DoD 5200.1-R, Information Security Program Regulation, Chapter IX. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Customer:	Joint Product Manager for Biological Detection Systems (JPM BDS)
Technical Monitor:	Mr. Christopher E. Hall Security Manager
Contract Numbers:	Reference Appendix C
Contract Office:	Reference Appendix C
TD Number(s):	0001
Security Classification:	UNCLASSIFIED
Title:	Operations Security (OPSEC) Plan

Approved by: ____ _______________

DENNIS A. CARD, Ph.D. Date
LTC, CM
Joint Product Manager
Biological Detection Systems

TABLE OF CONTENTS

1. PURPOSE (U)

(U) This Operations Security (OPSEC) Plan applies to all members managed by the Joint Product Manager for Biological Detection Systems (JPM BDS or BDS) programs including JPM BDS Government employees, Science Engineering Technical Assistance (SETA) Support Contractors, prime service contractors and their subcontractors who generate or handle Critical Program Information (CPI), as well as all other forms of sensitive information. It serves to identify and protect sensitive program-generated information and activities by:

- Presentinga documented methodology for denying adversaries the opportunity to collect BDS CPI.
- Identifying those sensitive aspectsof interest to adversaries and the procedures designed to eliminate and correct vulnerabilities that are susceptible to exploitation.
- Establishing policies, procedures, and responsibilities for the implementation of the OPSEC Program.

1.1 Scope (U)

(U) This OPSEC Plan applies to the activities of all BDS organizational elements. This plan is applicable to all current and future contractors involved with JPM BDS. See Appendix C for a list of current applicable contractors. The BDS OPSEC Working Group will provide additional guidance to those organizations not familiar with the aspects of OPSEC or the BDS OPSEC Program.

1.2 Legal and Regulatory Authorities (U)

5 U.S. Code (USC) 301 – Departmental Regulations
DoD Regulation 5200.1-R – Information Security Program
DoD Directive 5205.2 – DoD Operations Security Program

DoD Regulation 5220.22 – National Industrial Security Program Operating Manual (NISPOM)
DoD Directive 5400.7 – FOIA Program
DoD Regulation 5400.7-R – DoD FOIA Program
DoD Regulation 5400.11-R – Department of Defense Privacy Program

2. PERSONNEL RESPONSIBILITIES (U)

2.1 BDS Program Security Manager (U)

(U) JPM BDS Program Security Manager will ensure OPSEC considerations are given the highest priority and implement an OPSEC training program. The Joint Product Manager Biological Detection Systems (JPM-BDS) will provide guidance and oversight of the OPSEC Program.

2.2 OPSEC Working Group (U)

(U) The BDS OPSEC Working Group has been established to identify and resolve programmatic OPSEC issues that impact BDS. This working group will meet quarterly, or as necessary, to review this plan and is applicability to JPM BDS. Members of the working group consists of, but not limited to:

- Joint Product Manager, Biological Detection Systems
- BDS Program Security Manager
- Team Leader, Biological Integrated Detection Systems (BIDS)
- Team Leader, Joint Biological Point Detection System (JBPDS)
- Team Leader, Joint Portal Shield (JPS)
- Team Leader, Joint Biological Stand-off Detection System (JBSDS)
- Team Leader, Joint Biological Tactical Detection System (JBTDS)
- Implementation Team Member

(U) As mission and situation dictates, additional personnel (i.e., Information Assurance, Finance, Contract Representatives) may be called upon to address specific issues and provide subject matter expertise to the working group.

3. GENERAL APPLICABILITY (U)

(U) The OPSEC Plan is a set of procedures and methodologies implementing cost-effective measures for the protection of CPI. The OPSEC Plan provides a process of analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems.
- Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- Select and execute measures that eliminate or reduce, to an acceptable level, the vulnerabilities or friendly actions to adversary exploitation.

4. SPECIFIC THREATS TO BDS (U)

(U) OPSEC deals with the development of countermeasures to protect information and to eliminate and minimize indicators. It is important to understand that OPSEC deals mainly with unclassified, sensitive CPI that when brought together and analyzed, could reveal classified information to potential adversaries or deny mission accomplishment.

(U) The proliferation of weapons of mass destruction (WMD) continues. At least 20 nations maintain or have the capability to develop biological weapons. Biological weapons (BW) are an asymmetric counterbalance to U.S. sophisticated precision guided weapons and force protection capability. State run WMD is a serious threat to the US. In addition, these programs are a potential source for terrorists to acquire and employ biological weapons and CBRN hazards against both Continental United States (CONUS) and Outside CONUS (OCONUS) installations and facilities.

(U) BW agents pose unique challenges because they are relatively easy to produce, difficult to detect, and their production facilities have no unique signature. The potential lethality of biological versus chemical agents by weight and relative low costs make BW agents an attractive alternative. Effective dissemination can be achieved using readily available commercial technologies such as agricultural or industrial sprayers. Threat biological agents include bacterial viruses and toxins. JPM BDS will use the current ITF 6 Category A agent list for the determination of BW agent threat.

5. OTHER THREATS TO BDS (U)

(U) The worldwide intelligence collection threat is multi-disciplined, highly sophisticated, and extremely dedicated. Intelligence collection efforts may use only one discipline or a combination of disciplines to obtain information. OPSEC is not a replacement for traditional security programs, nor is it a management tool for these programs; rather it integrates their efforts and thus ensures essential secrecy. As new threat data is received, distribution shall be made to BDS personnel and others as appropriate.

5.1 Human Intelligence (U)

(U) Human Intelligence (HUMINT) is the discipline of intelligence collection in which humans serve both as collectors and sources of information. They may reveal their own knowledge of a sensitive project or provide documentation to which they have access as a result of being in a position of trust.

(U) Most HUMINT collectors do not fit the image of ***the spy***. Rather they may be students, businessmen, and attendees at conferences or seminars or even tourists. Seemingly innocent relations with foreign nationals have turned into espionage recruitment situations. Initially unwitting to the recruitment process and ulterior motives of the case officer, individuals may be convinced to provide unclassified information and then coerced or enticed with cash to provide more valuable information.

(U) HUMINT is collected primarily to anticipate military application of technological advancements and to foster scientific, mechanical, and industrial support of the collector's military and strategic forces. HUMINT against the BDS may include:

- Intelligence agents assigned to target and develop contacts with DoD and contractor personnel associated with the BDS.
- Foreign visitors with ulterior motives for collecting technical knowledge and information concerning the BDS.
- Professional conferences or symposia providing opportunities for adversaries to elicit and exploit personnel associated with the BDS. Engineers and scientists who are attending the conferences or symposia as a covert representative of an adversary typically accomplish exploitation. Collection efforts may range from innocuous questions to outright blackmail attempts. Without constant awareness of the threat, BDS personnel may inadvertently release sensitive information.
- Employee disaffection, although internal in nature, poses a threat to the BDS. Theft, malicious alternations of data, sabotage, espionage, and destruction of critical equipment and materials could cause serious damage to the BDS.
- Terrorism, carried out by militant domestic or foreign groups, poses a constant threat to military or contractor personnel, equipment, and operations.

(U) The HUMINT element poses a significant threat to sensitive functions of any program. The threat is considered to be continuous, applicable to all BDS activities and functions which could be conducted in an overt or covert manner. Vulnerabilities susceptible to collection include:

- Disclosure of sensitive technology transfer applications in technical publications, magazines, newspapers, or other media available to the general public.

- Dissemination of classified or unclassified test results to personnel without the need-to-know.
- Failure to truly evaluate the classification or sensitivity of information that would exempt it from release under the FOIA.
- Failure to follow published security guidance or regulations in the physical handling and storage of classified components.
- Inadvertent disclosure of classified or unclassified sensitive information.

5.2 Open-Source Intelligence (U)

(U) Open-Source Intelligence (OSINT) is a discipline of intelligence collection where collectors use verbal, written, or electronically transmitted material that can be legally acquired. The very best source of technical data is open-source information. More than 90 percent of all information gathered by a typical foreign intelligence effort about the U.S. and its activities is derived from open sources. It includes the acquisition of newspapers, magazines, journals, as well as monitoring broadcasts on commercial and public radio and television.

(U) Open-source literature supplies adversaries most of their intelligence requirements through the systematic collection and analysis of information available to the general public. Such information is commonly obtained through newspapers, the National Technical Information Center, the Defense Technical Information Center, meetings and seminars, and through contractor advertisements. These sources provide adversary analyses centers with highly valuable information regarding capabilities, limitations, and technical performances of our systems.

(U) Studying the journals in fields such as chemistry, physics, engineering, mathematics, optics, etc., can provide valuable insight into the level of sophistication a country has in a particular field. Examining articles written for open-source journals by a scientist known to be associated with that institute can gather information about the activities in a particular research institute. This can provide indicators to ongoing developments that perhaps are being applied to BDS hardware or software. The frequency with which researchers publish may provide insight into the formation of new research groups and the application of the research to future components. A sudden end of published reports may indicate a transition from basic to applied research and a new component. The Internet is a major resource for OSINT collectors so extreme caution should be given to this resource for OSINT indicators.

5.3 Signals Intelligence (U)

(U) Signals Intelligence (SIGINT) is intelligence derived from the interception, processing, and analysis of signals. Subsets of SIGINT include Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).

(U) SIGINT embraces all forms of radiating equipment including communications, telemetry, and microwave. A primary SIGINT target is the microwave telecommunications system (the unsecured telephone). All BDS personnel will be made aware during security awareness training that the majority of all telephone conversations are transmitted by microwave and are vulnerable to interception and exploitation unless protected by the use of Secure Telephone Unit/Secure Telephone Equipment (STU/STE) in the secure mode.

(U) COMINT, one of the primary SIGINT disciplines, includes information derived from intercepted communications transmission, including voice, facsimile and dial-in computer access lines. Interception of microwave transmission is possible by anyone with adequate receiving equipment. The targeting of e-mail and telephone or fax transmissions is of importance to the BDS. To collect telephone transmissions (voice and fax), dial number recognition is used. Numbers known to be associated with organizations or locations of interest are automatically collected both for content and to monitor the volume of calls, which are indicators of actual or pending activity. SIGINT can be collected from satellites, fixed ground stations, ships off the coastline, aircraft flying overhead, and from as close as a van parked in a nearby lot. In addition to gleaning intelligence, adversary operatives also monitor communications to exploit specific personal information that could be used to blackmail BDS personnel into committing acts of espionage or sabotage.

(U) Current technology has produced a situation in which telephones in the cradle (on-hook position) may frequently transmit room conversation occurring in the vicinity of the telephone. The telephone handset may act as a microphone that can pick up and transmit room electronic signals and voice. This may be the result of accidental or intended modification or because of a design characteristic of the telephone instrument or its associated equipment.

5.4 Imagery Intelligence (U)

(U) Imagery Intelligence (IMINT) is intelligence derived from the collection, processing, and analysis of images across the entire optical spectrum, including photo satellites; commercial and private aircraft; hand-held photography of documents, components, areas, etc.; and unauthorized use of copying, duplicating, or video equipment. IMINT can be collected from platforms on land, air, sea, and space. While IMINT agents still provide valuable imagery with hand-held cameras, the primary IMINT collection platforms are satellites and aircraft.

5.5 Intelligence Collection Threats to the BDS (U)

(U) There is a consensus within the U. S. Intelligence Community that almost all DoD exercises and operations are faced with intelligence collection threats. The Defense Security Services publication *Technology Collection Trends in the U. S. Defense Industry, 2004*, identifies that Information Systems (IS) remain the most sought after military critical technology with sensors, second only to lasers as the most frequently reported technology with foreign collection efforts.

6. CLASSIFIED INFORMATION (U)

(U) BDS has an established system of control measures which assure that access to classified information is limited to authorized persons. The system includes technical, physical, and personnel control measures.

(U) Information that is classified is often restricted in its dissemination based on the “need to know.” In order to have access to classified information, one must have both the appropriate clearance level and the need-to-know. Proper safeguarding of handling classified information can be found in the NISPOM. The following definitions describe the seriousness of both intentional and inadvertent disclosure if released to the public.

Secret – the second highest classification. Information is classified Secret when its release would cause “significant damage” to national security.

Confidential – is the lowest classification level. It is defined as information which would cause “damage” to national security if disclosed.

6.1 Special Considerations (Aggregation of Data) (U)

(U) Aggregation of data is the compilation of unclassified individual data systems and data elements resulting in the totality or order in which the information is displayed being classified. It is important to re-emphasize that aggregation of data is one of the primary focal points of the JPM BDS’s protection methodology. For example, when an installation’s specific critical missions are compiled in their entirety and the missions and critical infrastructure are prioritized, this list becomes classified Secret. An approved unclassified list would be a list in priority order beginning with the most critical and ending with the least essential (but not labeled as such) and would include building facility, unclassified mission, and POC information for the facility.

7. FOR OFFICIAL USE ONLY INFORMATION (U)

(U) For Official Use Only (FOUO) is a designation that is applied to *unclassified* information that may be exempt from mandatory release to the public under the

Freedom of Information Act (FOIA). The FOIA specifies nine exemptions which may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. They are:

1. Information which is currently and properly classified.
2. Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles, “high” and “low.” The “high” profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The “low” profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)
3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.
5. Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.
6. Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
7. Records or information compiled for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to a fair trial or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others, (d) disclose the

identity of a confidential source, (e) disclose investigative techniques and procedures, or (f) could reasonably be expected to endanger the life or physical safety of any individual.

8. Certain records of agencies responsible for supervision of financial institutions.
9. Geological and geophysical information concerning wells.

(U) Information that is currently and properly classified can be withheld from mandatory release under the first exemption category. “For Official Use Only” is applied to information that is exempt under one of the *other* eight categories. So, by definition, information must be unclassified in order to be designated FOUO. If an item of information is declassified, it can be designated FOUO if it qualifies under one of those other categories. This means that (1) information cannot be classified and FOUO at the same time, and (2) information that is declassified may be designated FOUO, but only if it fits into one of the last eight exemption categories (categories 2 through 9).

(U) The FOIA provides that, for information to be exempt from mandatory release it must fit into one of the qualifying categories *and* there must be a legitimate Government purpose served by withholding it. Simply because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information must be reviewed to see if it meets this dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of records (for example, personnel records) are not normally marked FOUO, but may still qualify for withholding under the FOIA.

7.1 Safeguarding FOUO (U)

(U) The Department of Defense (DoD) defines what information shall be protected and how the protected information shall be handled. FOUO information should be handled in a manner that provides reasonable assurance that unauthorized persons do not gain access.

7.1.1 Access to FOUO Information (U)

(U) Access to FOUO material shall be limited to those employees needing the material to do their jobs. FOUO information may be disseminated within the DoD and between officials of the DoD and DoD contractors.

7.1.2 Marking FOUO Information (U)

(U) Contractors supporting the BDS are authorized to mark correspondence and other forms of documentation as FOUO in accordance with the BDS Security Classification Guide (SCG) and this OPSEC Plan. Unclassified documents and material containing FOUO information shall be marked as follows:

- An unclassified document containing FOUO information will be marked FOR OFFICIAL USE ONLY in letters larger than the rest of the text, where practical.
- Documents will be marked FOR OFFICIAL USE ONLY at the bottom of the front cover (if there is one), the title page (if there is one), the first page, succeeding pages, and the outside of the back cover (if there is one).
- Material other than paper documents (e.g., slides, computer media, films, etc.) shall bear FOUO markings, which alert the holder or viewer that the material contains FOUO information.
- Within a classified document, an individual page that contains FOUO and classified information will be marked at the top and bottom with the highest security classification appearing on the page.
- Only the originator or other competent authority can accomplish removal of the FOR OFFICIAL USE ONLY marking. When FOR OFFICIAL USE ONLY status is terminated, all known holders will be notified by the appropriate JPM BDS authority.

7.1.3 Storage of FOUO Information (U)

(U) During working hours, FOUO material must be placed in discreet locations if work areas are accessible to persons who do not have a valid need to know for the material. This process should be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO material should be placed in locked containers, desks, or cabinets or kept in locked offices.

7.1.4   Mailing (U)

(U) FOUO information may be sent via first-class mail or parcel post. Bulk shipments can be sent fourth-class mail.

7.1.5   Electronic Transmission via Fax (U)

(U) The sender will coordinate with the recipient to ensure that the material faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.

7.1.6   Transmittal via E-Mail (U)

(U) FOUO information transmitted via e-mail should be protected by encryption. For added security, when transmitting FOUO over a regular email channel, the information can be included as a password protected attachment with the password provided with a subsequent email. Recipients of FOUO information will comply with any e-mail restrictions imposed by the originator. FOUO may **NOT** be transmitted through e-mail using a personal e-mail account (e.g., .net, hotmail) on the Internet.

7.1.7   Internet (U)

(U) FOUO information will not be posted on any internet (public) website. FOUO information may be posted on the Integrated Digital Environment (IDE). However, the individual posting information should be aware that access to the information is open to all personnel who have been granted access to that particular network. The individual must determine the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as FOR OFFICIAL USE ONLY; and information posed does not violate any provisions of the Privacy Act.

7.1.8 Disseminating FOUO (U)

(U) Contractors may disseminate FOUO information to their employees and subcontractors who have a valid need-to-know for the information in connection with this contract.

7.1.9 Disposal and Unauthorized Disclosure of FOUO (U)

(U) Protect and dispose of FOUO information in the same manner as company-proprietary information or in a way that will prevent disclosure of contents or reconstruction of the material (secure lockable destruction bins). The unauthorized disclosure of FOUO material is not an unauthorized disclosure of classified information. However, DoD contractor personnel have a duty to take reasonable actions to protect FOUO material under their control from unauthorized disclosure. Appropriate administrative actions should be taken to address responsibility for such disclosures. Unauthorized disclosure of FOUO information protected by the Privacy Act may also result in civil or criminal sanction against DoD and/or the BDS Team.

7.2 Distribution Statement D for Use on Technical Documents (U)

(U) All technical documents within the BDS including working papers, memoranda, and preliminary reports, if not already in the public domain, and if they are likely to be disseminated outside of DoD, shall be marked with Distribution Statement D. All material containing technical information generated for the BDS shall be marked on the face of the document, or cover/title page. All JPM BDS technical documents shall bear the following Distribution Statement:

DISTRIBUTION STATEMENT D – Further dissemination only as directed by Joint Product Office Biological Detection Systems or higher DoD authority.

7.2.1 Definition (U)

(U) Distribution Statement D marking is distinct from and in addition to a security classification marking assigned in accordance with Army Regulation (AR) 380-5/DoD 5220.22-M. Reasons for assigning Distribution Statement D include:

- Administrative or Operational Use.To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical papers, technical reports and other publications containing valuable technical or operational data.
- Critical Technology. To protectinformation and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoD Directive 5230.25.

- Specific Authority. Toprotect information not specifically included in the above reasons, but which requires protection in accordance with valid documented authority such as Executive Orders or classification guides.

7.3 Enforcement (U)

(U) Administrative penalties may be imposed for misuse of FOUO information. Criminal penalties may be imposed depending on the actual content of the information (privacy, export control, etc.).

8. CRITICAL PROGRAM INFORMATION (U)

(U) Identifying critical program information (CPI) is the first step to reaching optimum protection. DoD Directive 5205.2 (DoD Operations Security (OPSEC) Program) defines CPI as "specific facts about friendly intentions, capabilities, operations, and other activities vitally needed by adversaries for them to plan and act effectively, so as to guarantee failure or unacceptable consequences for friendly mission accomplishment." The BDS CPI includes:

- Critical Reagent Program(CRP) Products. Biological detection sensors use reagents and immunoassays furnished by the CRP. The reagents/assays are designed to identify specific biological weapons. Reagents are coded to conceal agent affinity—the ability of CRP agents to detect biological agents when deployed on-site at an installation including the actual agents and the detection levels for the system.
- Disclosure of critical elementswithin reagents/assay production. The sequences and target specificities of the probes as well as nucleic acid sequences. Detailed information relating to the structural characteristics of those targets could allow adversaries to genetically engineer biological weapon agents that could no longer be detected with our current reagents and equipment.
- The ability of CRP agents to detect biological agents when deployed on-site at an installation including the actual agents and the detection levels for the system.
- Disclosure of critical elements within reagents/assay information in the form of specific target sequences and target specificities of the probes as well as nucleic acid sequences. Detailed information relating to the structural characteristics of those targets could allow adversaries to

genetically engineer biological weapon agents that could no longer be detected with our current reagents and equipment.

- Antibody Target Information.
- Gene sequence information.

(U) A preliminary list of CPI was developed through discussions with JPM BDS personnel, BDS Security Classification Guide (SCG), and a review of the existing CRP. JPM BD contacted the Joint Program Executive Office for Chemical and Biological Defense (JPEOCBD) to identify and verify CPI listed in the SCG for specific products. The results showed that the CRP was critical to any adversaries' intent on exploiting BDS for their own purposes.

8.1 CPI and the Threat (U)

(U) Identifying CPI is a team effort. Managers are encouraged to include their subject matter experts (security personnel, engineers, team leaders) as part of the process when identifying CPI. Accurate threat assessments are dynamic and change based on the BDS equipment status. As BDS technology matures and the CPI transitions, protection must be adjusted accordingly.

8.2 OPSEC Indicators (U)

(U) Indicators are observable or detectable activities or information that can be pieced together to reveal sensitive information regarding your operation. They act as clues to an activity that adversaries can exploit to their advantage through analysis. They include such things as: travel orders, identification of key personnel, movement of equipment that can be observed; conversations and readable documents. All detectable indicators that convey or infer CPI must be identified and protected.

(U) Caution must be taken not to provide information that could serve as indicators to identify friendly intentions, capabilities, and activities which could:

(1) Diminish the effectiveness of operations or activities,

(2) Compromise classified or sensitive unclassified information or activities,

(3) Provide various adversaries or competitors with information allowing technological, tactical, or strategic advantage,

(4) Diminish the effectiveness of a security program or plan in effect

(U) Following is a list of indicators that might, by observation, aggregation, deduction, inference or other exploitation disclose critical information about the BDS.

8.2.1 Operations Indicators (U)

- BDS Schedules (Example: BDS Integrated Master Schedule).
- Visits/Meetings of BDS personnel associated with particular activities (i.e. site survey, design, fielding, and logistics).
- Abrupt changes or cancellations of meetings and schedules.
- Purchase of BDS Equipment.
- Sending BDS personnel for increased program related training.
- Increased volume of telephone calls, conferences, and longer working hours (including weekends).
- Increased volume of purchase or delivery of take out food to BDS offices after hours.
- Unusual or increased levels of trips and conferences by BDS personnel.
- Implementing procedures (Technical Directives and associated BDS documents).
- BDS system operational hours (when the system is actually conducting surveillance).
- Aspects specifically associated with the various systems operational modes.

8.2.2 Communications Indicators (U)

- BDS activity that results in nonsecure transmission of sensitive or classified information that should be passed over secure communications (voice, fax, computer).
- Talking around a sensitive or classified subject.
- Discussing classified or sensitive BDS information over non-secure communications (voice, fax, and computer).
- Insisting that sensitive or unclassified information be passed over non-secure telephone, facsimile, or computer to inform or brief senior officials.
- Arranging the itinerary of senior officials over non-secure communications (voice, fax, and computer).

8.2.3 Administrative Indicators (U)

- Travel Orders.
- Convening of planning and pre-execution conferences.
- Distinctive emblems or logos; marking on personnel, equipment and supplies.
- Transportation arrangements.
- Memorandums/advance plans.
- Posting of schedules, orders, plans, agendas, rosters, etc.
- Leave cancellations and restrictions.
- New facility activations.
- Press releases, brochures, reports.
- Identifiers.
- BDS unique abbreviations/acronyms.
- Nicknames.
- Mail volume.

8.2.4 Logistics/Maintenance Support Indicators (U)

- Volume and priority of requisitions/orders.

- Storing boxes or equipment with the name of the program or program activity outside a controlled area.
- Pre-positioning and establishment of logistics bases/warehouses.
- Procedural disparities in requisition and handling.
- “Crash” maintenance and logistics activity.
- Unusual equipment modifications.
- Deviations or special logistics support procedures.
- Providing unique or highly visible physical security arrangements for loading or guarding special equipment or facilities.
- Specialized vehicles and equipment.
- Movement nodes/choke points.
- Failure rates.
- System-wide deficiencies.
- Inventory.
- Requirements.
- Demand.
- Shelf life time.
- Equipment/parts availability.
- Storage capacity.

8.2.5 Planning Activity Indicators (U)

- Exercises and scenarios.
- Physical security.
- Planned activity profile.
- Security Classification Guides.
- Sensor capabilities.

8.2.6 Financial Activity Indicators (U)

- Budget analysis.
- Budget justification documents.

- Budget projections & estimates.
- Financialplans.
- Operatingbudgets.
- TDY funds requirements/limits/usage.
- POMinputs.
- Travelvouchers.

8.2.7 Personnel Activity Indicators (U)

- Manpower/strengthprojections.
- Training.
- Skillshortages.
- Specialmanning.
- Special skills requirements.

8.2.8 Design and Services Support Indicators (U)

- Designfactors.
- UtilityRequirements.
- EnvironmentalImpact.
- Firefightingcapabilities.
- Roadusage.
- Trashdisposal.
- Newconstruction.
- Camouflage.
- Structuremodifications.
- Facilitymaintenance/usage.
- Agent/simulantcorrelations.

9. COUNTERMEASURES OVERVIEW (U)

(U) Vulnerabilities of the various BDS operations may reveal sensitive or classified information, plans, or activities. Risk is a measure of the probability that an adversary will be able to exploit vulnerability and the impact to the program. Analysis of vulnerabilities identifies what measures or countermeasures are required to safeguard information. The most desirable OPSEC measure combines the highest protection with the least impact on BDS effectiveness.

(U) BDS personnel will use continual education and training to mitigate vulnerabilities discovered through ongoing OPSEC analysis. Participants shall be briefed and kept informed of all sensitive aspects of the operation and the measures designed for the protection of this information and the need for continued awareness and enforcement of OPSEC principles. Personnel will be briefed concerning the OPSEC significance of their day-to-day tasks as the activities and operations are undertaken to support the BDS.

9.1 Open-Source Literature (U)

(U) Even unclassified information released to the news media or at meetings or planning sessions may provide analytical centers with valuable information regarding individual system capabilities, limitations, and operations. Presentations by BDS individuals at symposiums or conferences in their area of expertise can make this individual a target to obtain further information.

9.1.1 Countermeasures (U)

(U) Procedures are in place to ensure no public release concerning BDS information occurs without prior written approval. An OPSEC reviewed of all information is to be completed as part of the review cycle. All presentations at symposiums or conferences will require review through the BDS public release process prior to disclosure.

9.2 Communications and Transmission (U)

(U) All unsecured telephone conversations (including cellular phones) are especially vulnerable to monitoring and all long distance microwave transmissions are subject to interception. These vulnerabilities provide a source of information for intelligence agents. Communications supporting IS and faxes are equally vulnerable. Mailing program Controlled Unclassified Information (CUI) makes it susceptible to interception or loss.

9.2.1 Countermeasure (U)

(U) Emphasis will be placed on instilling awareness among program participants concerning the use of communication devices. Discussions of classified nature via unsecured telephones are absolutely prohibited. It is incumbent upon each individual to exercise prudent telephone security when using unclassified company telephones. CUI should be faxed via secure means when possible. Classified information will only be transmitted in accordance with DoD Directive 5200.1-R, Chapter 7 and the NISPOM, Chapter 5, Section 4.

9.3 Information Systems Operations (U)

(U) Without adequate security measures, IS are susceptible to intrusion or tampering through both hardware and software manipulation. The emanations from IS equipment and power lines may be subject to interception. Electronic equipment such as computers may produce emanations that are susceptible to interception.

9.3.1 Countermeasure (U)

(U) All classified processing is performed on IS with removable hard drives to be secured in a General Services Administration (GSA) container when not in use in a secure area with restricted entry. An adversary would need to gain access to the GSA container or secure area to retrieve the IS media. Classified computing systems will have the required password protection screensaver function operating that will activate after 10 minutes of inactivity on the IS. CUI being transmitted over unclassified computing systems must be encrypted with 128-bit encryption in accordance with DD Form 254. Personnel are encouraged to utilize the JPEO CBD Integrated Digital Environment (IDE) for the sharing of CUI files.

9.4 Visitor Control (U)

(U) Visitors to any/all facilities may observe or hear sensitive information, operations, or activities.

9.4.1 Countermeasure (U)

(U) All visitors to an area where classified information is stored, processed, or discussed fall under two categories: cleared and uncleared. When an uncleared individual enters a closed area, all processing and discussion stops until the uncleared individual departs the area. Visitors are required to process through established checkpoints for verification of identity, citizenship, personnel security clearances, appropriate certification of purpose of visit, issuance of badges, and inspection of articles being brought into and out of the facility. Verification of Personnel Security Investigations, Security Clearances and affiliation of visitors will be done thru the Joint Personnel Adjudication System (JPAS).

(U) BDS personnel must be very diligent about being aware of other visitors in unclassified program areas such as janitorial personnel and maintenance personnel. CUI will be protected and properly maintained during such visits. Escort for visitors shall be advised of proper escort procedures, limitations on disclosure, and other applicable controls involved in the visit.

9.5 Conference Room Security (U)

(U) Classified and sensitive information could be compromised by covert listening devices installed in meeting rooms frequently used for sensitive discussions, or by overt measures of individuals listening in thru doors, windows, etc.

9.5.1 Countermeasure (U)

(U) All conference facilities are maintained as secure areas. Access to these facilities by uncleared individuals requires an escort at all times. No uncleared individual is left alone in these conference facilities. BDS personnel will be reminded of conference room procedures when discussing classified or sensitive but unclassified program matters. This will include attendance control, procedural security information while the conference is in session, instructions on note taking, disclosure of the classification or sensitivity of information being discussed, and procedures to ensure that all material is protected during the sessions, including breaks, and at the end of sessions.

9.6 Disgruntled Personnel and Personnel with Personal Problems (Adverse Information) (U)

(U) All personnel possessing security clearances whom, through personal adversities or circumstances such as marital difficulties, criminal behavior, excessive indebtedness or indiscriminate use of alcohol, present attractive targets to Hostile Intelligence Service (HOIS). Supervisors or fellow employees may become aware of these difficulties but may fail to notify management or security to investigate, electing to ignore the problem or rationalizing that some other party will take action. Non-action on the part of personnel who become aware of these situations can be as significant as that presented by an adversary who may attempt to exploit personnel experiencing these problems.

9.6.1 Countermeasure (U)

(U) BDS personnel are continually trained to report suspicious behavior or potential security issues to JPM BDS, security, and their management.

10. OPSEC PROCESS (U)

(U) The OPSEC process focuses on the protection of information and operations from unauthorized disclosure of the BDS, to adversaries and others who do not have a need to know for the information. The process also helps prevent or reduce the inadvertent release of operational information to these same adversaries. OPSEC is a five-step process that entails:

- Identification of citical information.
- Analysis of threats.
- Analysis of the vulnerabilities.
- Assessment of risks.
- Applicationof OPSEC measures.

10.1 Identification of Critical Information (U)

(U) Based on the BDS and applicable SCG, JPM BDS Security Manager will determine operational specific critical information to be surveyed. This serves to focus the OPSEC Process on protecting the vital information, rather than attempting to protect all information.

10.2 Analysis of Threats (U)

(U) This involves the research and analysis of reports, and open source information to identify who the likely adversary could be. Questions to be asked are discussed in the following paragraphs.

10.3 Analysis of Vulnerabilities (U)

(U) This action identifies the BDS operation vulnerabilities. This requires examining the parts of the planned operation and identifying OPSEC indicators that could reveal critical information. Vulnerabilities exist when an adversary is capable of observing an OPSEC indicator, correctly analyzing it, and then taking appropriate and timely action.

Reviewing results of preparations (workups) to the operation such as sensor location will help identify vulnerabilities not readily apparent.

10.4 Assessment of Risk (U)

(U) This step essentially has two components. First, planners analyze the identified vulnerabilities and then identify possible OPSEC measures against them. Second, specific OPSEC measures are selected for execution based on the risk assessment done by the BDS Security Staff. OPSEC Measures can be used to:

- Prevent compromise to an OPSEC indicator.
- Intentional deviations from normal patterns; and conversely, providing a sense of normality.
- Practicing sound information security, physical security, and personnel security.
- More than one OPSEC measure may be identified for each vulnerability; and one OPSEC measure can be identified for multiple vulnerabilities.
- Primary and secondary OPSEC measures can be identified for single or multiple OPSEC indicators.
- OPSEC measures are most effective when they provide the maximum protection while minimally effecting operational effectiveness.

(U) Risk assessment involves comparing the estimated cost (time, effort, resource allocation, and money) of implementing an OPSEC measure to the potential effects on mission accomplishment resulting from compromise of a particular vulnerability.
More than one OPSEC measure may be identified for each vulnerability, and one OPSEC measure can be identified for multiple vulnerabilities. Primary and secondary OPSEC measures can be identified for single or multiple OPSEC indicators. OPSEC measures are most effective when they provide the maximum protection while minimally effecting operational effectiveness.

(U) Risk assessment involves comparing the estimated cost (time, effort, resource allocation, and money) of implementing an OPSEC measure to the potential effects on mission accomplishment resulting from compromise of a particular vulnerability.

(U) Planning for OPSEC measures requires coordination amongst all staff elements, and supporting elements or assets outside the BDS. Particular care must be taken to ensure that OPSEC measures do not interfere with other operations. Solid staff functioning and planning will ensure OPSEC plans integrate with and support other Bases, programs and operations.

10.5 Application of OPSEC Measures (U)

(U) In this step, the BDS Security staff implements the OPSEC measures selected in the previous step (Risk Assessment). Planning and integrating OPSEC measures into the BDS is critical to ensure counter measures are applied at the right time, place, and manner. In addition to ongoing operations, feedback provides information for OPSEC planning for future operations through “lessons learned.” The OPSEC Survey is an excellent method and tool for providing feedback on the effectiveness of OPSEC measures.

11. OPSEC SURVEY (U)

(U) The OPSEC survey is an intensive application of the OPSEC process to our operation by a multi-disciplined team of experts. The BDS should tailor the survey to their specific requirements. To begin the survey, critical information must be identified. Without critical information, a determination that vulnerabilities exist cannot happen. The OPSEC survey determines if the critical information is being protected. OPSEC surveys evaluate the OPSEC measures and if needed, recommend changes to existing measures. The survey can also identify requirements for additional OPSEC measures. The purpose of the OPSEC survey is to determine if adequate protection exists. The survey will determine if critical information is being protected. The critical information has to have been identified during the OPSEC process for this to happen. The BDS

Security Manager shall perform surveys on all facilities to include subcontractor's annually.

(U) OPSEC surveys differ from security inspections in that security inspections seek to ensure compliance with directives and regulations concerning classified or unclassified material, and security of physical structures and facilities. However, survey teams should also ensure that security measures are not creating OPSEC indicators. Surveys are not to be used as a punitive tool, but should be conducted on a non-attribution basis. This will ensure better cooperation and honesty when surveying the BDS activities, plans, and operations.

(U) Results of OPSEC surveys should be given to the BDS Program Security Manager. All BDS survey results shall be forwarded to the JPM BDS Security Manager.

(U) OPSEC surveys will be accomplished by a formal survey. An OPSEC survey is conducted by members within the JPM BDS BDS security program staff. The OPSEC Survey is composed of the following phases (planning, field survey, analysis and reporting).

12. OPSEC AWARENESS TRAINING (U)

(U) For the BDS OPSEC to be effective, all persons assigned to or associated with the organization the concepts of OPSEC, and apply that knowledge and awareness in the performance of their day-to-day tasks. OPSEC training programs, to be meaningful over the long term, is action and job oriented being relevant to the tasks assigned. The content of material presented is directed to answer three primary questions the audience is likely to ask:

1. Why is OPSEC important to JPM BDS Defense?
2. Why is OPSEC important to me?
3. How can I contribute to OPSEC?

(U) OPSEC orientation will be provided to individuals within the first 10 days of arrival in the BDS. JPM BDS has instituted OPSEC briefing materials to address OPSEC concerns, see Appendix B.

(U) Focus of the training includes an overview of the OPSEC threat to the operation; the role of OPSEC in supporting operations planning and execution and provisions of the JPM BDS program.

(U) All BDS Security Officers to include contractors and sub-contractors will provide periodic reminders of the importance of sound OPSEC practices needed to deny or control information about organizational capabilities and intentions from compromise, in the form of annual security training and awareness program.

APPENDIX A
ACRONYMS/ABBREVIATIONS (U)

AR	Army Regulation
BDS	Biological Detection System
COMINT	Communications Intelligence
CPI	Critical Program Information
CUI	Controlled Unclassified Information
DoD	Department of Defense
EEFI	Essential Elements of Friendly Information
ELINT	Electronic Intelligence
FISINT	Foreign Instrumentation Signals Intelligence
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GFE	government-furnished equipment
GSA	General Services Administration
HOIS	Hostile Intelligence Service
HTTPS	Hypertext Transfer Protocol - Secure
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
BDS	Installation Protection Program
IS	Information Systems

JPM BDS	Joint Product Manager for Biological Detection Systems
MASINT	Measurement and Signatures Intelligence
NISPOM	National Industrial Security Program Operating Manual
OGA	Other Government Agency
OPSEC	Operations Security
OSINT	Open-Source Intelligence
PPT	Program Protection Team
SCG	Security Classification Guide
SIGINT	Signals Intelligence
STE	Secure Telephone Equipment
STU	Secure Telephone Unit
USC	U.S. Code

APPENDIX B

BIOLOGICAL DETECTION SYSTEMS OPSEC BRIEFING (U)

(U) The accomplishment of this annual requirement can be completed by two different methods. The majority of the organization will receive their training as part of the annual Aberdeen Proving Grounds, Security Awareness Training class, held multiple times during the FY. This training is no cost to JPM BDS as all tenant activities of APG participate in this training.

(U) The other method of training is available thru the BDS Security Manager. The Security Manager will provide the Interagency Operations Security Support Staff (IOSS) created OPSEC Fundamentals (OPSE 1301) course. This course is on CD and a certificate will be provided upon successful completion of the final exam. The BDS OPSEC Working Group will complete this course, in addition, to the annual APG training event.

APPENDIX C

CONTRACTS AFFECTED BY THIS OPSEC PLAN (U)

CONTRACTOR	CONTRACT NUMBER	CONTRACT OFFICE
GD-ATP (ISP)	W911SR-04-C-0017	Edgewood Procurement
GD-ATP (ISS)	W911SSR-05-D-0002	Edgewood Procurement
Harris Corp	W911SR-04-P-0618	Edgewood Procurement
Texas A&M	DAAD13-03-C-0050	Edgewood Procurement
SESI	W911SR-04-C-0020	Edgewood Procurement
BSM	W9113M-06-P-0013	Edgewood Procurement
Battelle (Carrier)	DAAD13-03-C-0018	Edgewood Procurement
AAI Engineering Spt Services	W52H09-04-D-0131	TACOM
AM General	DAAE-07-01-C-S001	TACOM
UT	N00024-01-D-6600	Navel Sea System Command
JHU	N00024-03-D-6606	Navel Sea System Command
Camber	N00174-02-D-0014	NAVSEA, Indian Head
Sentel	N00178-01-D-3019	Naval Surface Warfare Center
GD-Armament	W91ZLK-05-F-0176	APG Procurement
Chenega Tech Products	DAAB07-03-D-H605	CECOM
ARO	DAAD19-02-D-001	RDECOM, NC
SAS	DASG60-03-D-0001	Ft. Detrick Procurement
PM FBCB2	W15P7T-04-D-G2040	Northrup Grumman
VIC-3	DAAB07-02-D-0001	Northrup Grumman
SAIC	W9113M-05-F-0018	Ft. Detrick Procurement
RTI	W911SR-04-D-0012	Edgewood Procurement