State of New Jersey
DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
POST OFFICE BOX 340
TRENTON, NEW JERSEY 08625-0340

☆☆

JON S. CORZINE
Governor
Commander-in-Chief

GLENN K. RIETH
Major General
The Adjutant General

DEPARTMENTAL DIRECTIVE **1 May 2006**
NO. 25.2.3

INFORMATION SECURITY PROGRAM (IASD-ISB)

1. PURPOSE

The purpose of this policy is to set forth guidelines for the Information Security Program within all New Jersey Department of Military and Veterans Affairs (DMAVA) locations and facilities.

2. APPLICABILITY

This policy applies to all state employees, contract employees, hourly employees, offices and agencies within the New Jersey Department of Military and Veterans Affairs (DMAVA.

3. REFERENCES

- HQDA Regulation 380-5 Department of the Army Information Security Program
- DA PAM 25-1-1 Information Technology Support and Services
- DMAVA Policy 09-2001
- DMAVA Operational Circular 06-2004
- DMAVA Security Policies and Procedures Guide

4. DEFINITIONS

a. **Chief Information Officer:** Senior Information Technology official for the department.

b. **Department:** means the New Jersey Department of Military and Veterans Affairs.

c. **CISO:** Chief Information Security Officer

d. **Employee:** means all state employees of the Department or agency whether full-time or part-time, and whether in the career service, executive service, or unclassified service. This term includes contracted employees, hourly employees, and interns.

e. **Employer:** means the Department of Military and Veterans Affairs.

f. **PSP:** Policies, Standards and Procedures. Written and Non-written Security policies, and standard operating procedures

g. **SOG:** Security Oversight Group (SOG) shall be the executive forum for oversight, and management of the Information Security Program

5. OBJECTIVE

This document affirms DMAVA's resolve to protect the information and information resources under its control and to formally establish an ongoing program to ensure the implementation of its Security Goals and Standards.

The Information Security Program, chartered by this policy, is a proactive response to the changes we've seen in the information technology landscape. The Program shall:

- Reinforce DMAVA's commitment to the security of the information and information resources with which it is entrusted by the citizens of New Jersey.
- Define responsibilities for performing information security duties.
- Define an infrastructure to achieve and maintain the CIO's information security goals.
- Oversee the implementation of security controls (both technical and non-technical) across the DMAVA organization.
- Provide the infrastructure for DMAVA's security compliance efforts.

To achieve the DMAVA's information security goals, the Information Security Program will span the areas of security involvement illustrated in Figure 1. The Information Security Program will horizontally span all DMAVA organizational units and vertically employ the unique skill sets within the unique units. The matrix management approach will minimize the cost to implement the Program and maximize the "buy-in" of the agency relative to information security so that everybody becomes a stakeholder in the program's success. Some information security functions will be accomplished at the IASD level, some at the directorate, facility or program level, and some at both levels.

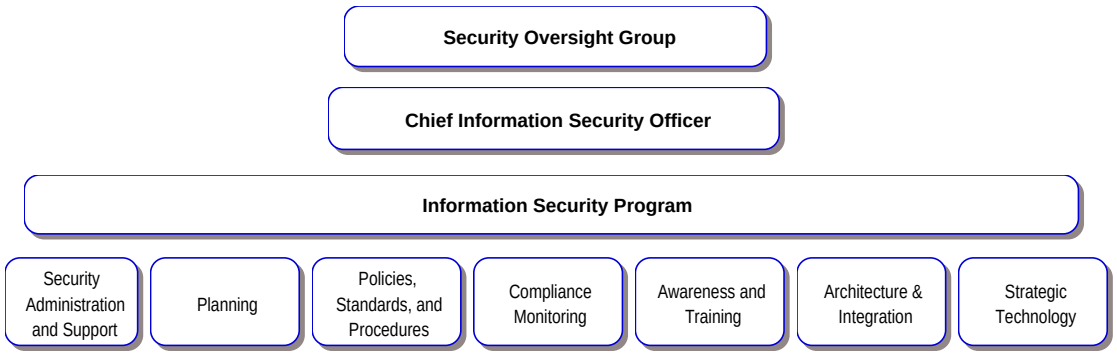

Figure 1. Areas of the Information Security Program.

6. POLICY

An Information Security Program shall be implemented within the Department of Military and Veterans Affairs (DMAVA) to ensure that current and future security goals and standards are/shall be appropriately implemented and maintained. The Chief Information Officer has established the following overriding information security goals for the New Jersey Department of Military and Veterans Affairs:

- Physical, technical, and administrative controls shall protect the confidentiality, integrity, and availability of information and information resources under DMAVA control.
- Information shall be protected against unauthorized access, while providing for public access as required by law.
- Security controls shall be established to not only prevent violations, but also to detect, contain, and correct violations.
- Legal, regulatory, and contractual requirements shall be met.
- Business continuity plans shall be produced, maintained, and tested.
- Information Security awareness and training shall be provided to all staff.
- Employees shall be held accountable for fulfilling their individual security responsibilities. Collectively, we shall be accountable for our performance as a team.

The Program shall be:

- Administered and monitored by a Chief Information Security Officer (CISO) with assistance from the Information Security Officer (ISO).
- Executed by all organizations within DMAVA so that pockets of organizational expertise work in concert to meet a common objective.

7. PROCEDURE

N/A

8. RESPONSIBILITIES

A. Chief Information Officer (CIO)

The Chief Information Officer has ultimate authority and responsibility for the approval, interpretation, implementation, and enforcement of all DMAVA Information Security Policies, Standards, and Procedures (PSPs) . The Chief Information Officer shall:

- Approve Information Security policies, standards, and procedures applicable to DMAVA as a whole or multiple DMAVA units. The Chief Information Officer may delegate this authority to the Chief Information Services Bureau.
- Appoint a Chief Information Security Officer (CISO) to oversee the Information Security Program on the CIO's behalf on a day-to-day basis.

- Delegate approval authority to Directors and CEO's for unit-specific Information Security PSPs (PSPs that are only applicable to their unit) that document unit-unique activities not covered by a dominant State or DMAVA PSP or unit-unique PSPs that supplement dominant State and/or DMAVA PSPs. Unit Heads shall not further delegate this authority.
- Elevate DMAVA PSPs for statewide consideration.
- Provide resources as appropriate/available to support the Program.
- Render a risk management decision on systems placed into the DMAVA operational environment to ensure that their utility is not overshadowed by the security risks of their use to DMAVA and New Jersey.
- Approve/disapprove requested exceptions to policy, standard, or procedure compliance. The CIO may delegate this authority.

B. Chief Information Services Bureau (ISB)

The Chief Information Services shall:

- Represent the Chief Information Officer and perform delegated authorities

C. Security Oversight Group (SOG)

A Security Oversight Group (SOG) shall be the executive forum for oversight and management of the Information Security Program within DMAVA. The Group shall be chaired by the CIO or a designee. The SOG shall consist of permanent (standing members) and non-permanent members and meet as a body on a prescribed basis. The SOG shall meet at least monthly to:

- Discuss, review, and approve information security policies, standards, and/or procedures brought before the Group for DMAVA adoption.
- Discuss, review, and set tactical (near term within a year) and strategic (long term up to five years) security strategies.
- Serve as an advisory body to the Chief Information Officer for security matters at the State (the "Enterprise") level.
- Provide oversight of Homeland Security initiatives and concerns.

Meeting minutes shall be documented and retained by the by the CISO.

1. Members

The standing membership of the SOG shall include the following at a minimum:

- Deputy Commissioner
- Chief Information Officer
- Chief Information Services Bureau
- Chief Information Security Officer
- Information Security Officer
- Senior Staff (e.g. Directors, CIO, Human Resources, Fiscal, Veterans Services, etc…,)
- Legal Council

- Facilities-Installations
- Others as specified by the Chief Information Officer

Note: Delegates sent to represent standing members of the SOG shall be empowered and expected to speak for and obligate the member they represent.

Non-permanent members can include:

- Subject Matter Experts (SMEs)
- Heads of Bureaus, Section or Units or their representatives
- Additional reviewers

By notifying the SOG meeting coordinator in advance, permanent members may invite non-permanent members to attend specific SOG meetings.

2. Responsibilities

Members of the SOG shall:

- Provide direction for security initiatives and activities.
- Ensure security initiatives are aligned with and enable business objectives.
- Actively promote the Information Security Program both internally and externally to DMAVA.
- Provide tactical (one year) and strategic (five year) direction for Information Security initiatives within DMAVA.
- Review, discuss, and recommend the approval (or disapproval) of DMAVA Information Security Policies, Standards, and Procedures (PSPs).
- Provide feedback and change recommendations to the Chief Information Security Officer on proposed policies, standards, and/or procedures that should be made prior to Group endorsement.
- Actively communicate with the CIO, the CISO, and other members of the SOG on Information Security Program matters.
- Nominate and furnish resources from their respective organizations to accomplish information security activities.

D. Chief Information Security Officer (CISO)

The Chief Information Security Officer shall:

- Manage the Information Security Program for the Chief Information Officer.
- Maintain a day-to-day awareness of all Information Security activities within DMAVA. Coordinate at all levels within DMAVA to ensure that the areas of security illustrated in Figure 1 are being addressed.
- Monitor information security activities throughout DMAVA. Work with project sponsors to identify project milestones where go-forward decisions are scheduled or appropriate. Review the information security aspects of the

project at the pre-determined milestones and provide the project sponsor with a security recommendation to assist with the go-forward decision. The CISO shall identify and assist in the resolution of security issues that could subject Units, DMAVA, or the State of New Jersey to an unfavorable security risk exposure. If security issues cannot be mutually resolved at the unit level, they shall be elevated to the SOG for resolution.

- Maintain an awareness of Homeland Security initiatives and issues at the DMAVA and State levels.
- Provide regular and ad hoc briefings on security matters to the CIO and SOG. Briefings should include the status of the Security Program, unit activities relative to information security, and/or security issues that require immediate attention/CIO intervention.
- Coordinate as appropriate, with personnel tasked with physical security responsibilities to ensure that physical security controls provide an acceptable level of protection for information and information resources.
- Represent the CIO, DMAVA, and New Jersey's information security interests at Homeland Security, industry standards committee meetings, technical conferences, etc.
- Work with public relations and senior management to develop public responses to information security inquiries.
- Create, sponsor, and/or support the creation of high-level policies applicable to multiple DMAVA units. The CISO shall be the focal point for PSPs that are applicable to multiple/all DMAVA business units. Unit Heads shall support the CISO to ensure that PSPs written for DMAVA-wide implementation reflect the desired baseline.
- Present proposed DMAVA-wide Information Security PSPs to the SOG for approval. The CISO shall provide recommendations with sufficient information so that the SOG can make an informed approval decision.
- Meet with all unit Information Security Coordinators (ISCs) on at least a quarterly basis to discuss information security issues.
- Provide information security recommendations to the CIO, SOG, and others to assist with informed risk management decisions.

E. Information Security Officer The Information Security Officer (ISO) shall:

- Assist and update the CISO as requested on the day-to-day awareness of security activities and issues within DMAVA.
- Assist the CISO with project monitoring and interface. Maintain contact and awareness, perform milestone security reviews, provide security recommendations, and conduct risk assessments on assigned projects.
- Identify and assist in the resolution of security issues that could subject Units, DMAVA, or the State of New Jersey to an unfavorable security risk exposure.
- Provide regular and ad hoc briefings on security matters to the CIO, CISO, SOG and others as requested.
- Represent the CISO, DMAVA and New Jersey's information security interests at industry standards committee meetings, technical conferences, etc.

- Provide assistance as required in support of policy, standard, and procedure development at the unit level. Provide timely review and response to Unit Heads on unit-unique PSPs.
- Direct the development of, or originate self-assessment activities, questionnaires, and other tools to assist Unit Heads with their security evaluation and compliance efforts.
- Maintain the CISO's library of relevant Information Security PSPs (State, DMAVA, and Unit-specific) and be the office of primary responsibility (OPR) for the content of DMAVA security PSPs.
- Provide content and delivery of an DMAVA Information Security Awareness program.
- Provide content and delivery of Initial Security Training for incoming personnel. To the extent possible, Initial Security Training should be accomplished in conjunction with other newcomer activities and prior to the employee being granted access to DMAVA information systems. All training shall be documented and attendance lists maintained. Awareness activities (posters, e-mail, mailings, etc.) do not require delivery documentation.
- Provide content and delivery for Annual Information Security Training.
- Monitor established forums for software vulnerabilities that could be exploited in the DMAVA environment. Bring the vulnerabilities to the attention of the applicable unit or units then monitor the unit's remediation efforts and progress.
- Conduct periodic spot-checks for PSP compliance.
- Coordinate the review and approval process of DMAVA PSPs.
- Attend Homeland Security meetings and monitor the status of Homeland Security initiatives and issues.

F. Directors, CEO's and Superintendents

Directors, CEO's and facility Superintendents shall:

- Ensure that all applicable Information Security PSPs (Federal, State, DMAVA and unit-unique) are being followed within their business units.
- Implement the appropriate levels of technical and non-technical support within their unit to address the areas of security illustrated in Figure 1 in relation to their unit's business case.
- Continually evaluate the implementation and effectiveness of technical and non-technical security controls to ensure the confidentiality, integrity, and availability of the information and information resources under their control. Self-evaluations that result in security concerns shall be elevated to the Chief Information Security Officer.
- As applicable, supplement, approve, provide training on, and maintain unit-unique documentation that reflects how their unit is implementing DMAVA PSPs if the implementation differs from DMAVA PSP requirements. (Units can make their PSPs more stringent than State or DMAVA PSPs but not less stringent. Units shall also create, approve, provide training on, and maintain unit-unique PSPs for which no dominant State or DMAVA PSP exists.) Note, <u>all</u> unit-unique PSPs (supplemental or unique) shall be reviewed and

receive concurrence from the Chief Information Security Officer before they are approved by the Unit Head.

- Furnish a current copy of all unit-unique security documentation to the Office of Security and Business Continuity Planning.
- Schedule annual and recurring security training for personnel within their unit. Unit Training shall be coordinated with the Information Security Officer and accomplished on an annual basis for all DMAVA employees or as necessary when there is a change in security procedures within the unit. All training shall be documented and attendance lists kept within the DMAVA Training Unit.
- Support the CISO and the Information Security Officer, with subject matter expertise and coordination as requested.
- Notify the CISO of all unit projects/initiatives that could have an information security component. Keep the CISO and/or the Information Security Officer in the project loop. Identify key milestones in the project plans where information security reviews and recommendations would be appropriate to support a go-forward decision process.
- Appoint an Information Security Coordinator (ISC) to be the directorate's focal point for information security issues and coordination. For example, the ISC would coordinate unit-specific policy development and review, as well as act as the liaison for DMAVA-wide policies that are developed by, or apply to, the unit. Contact information for the ISC's shall be sent to the CISO and the Information Security Officer. The ISC position shall be an additional duty position unless specifically approved by the CIO.

G. Fiscal, Legal, and Legislative Affairs

Fiscal, Legal, and Legislative Affairs provides their services to the Information Security Program on an as-required basis. Such services may include:

- Identify legislative requirements.
- Render legal opinions as appropriate (e.g., prosecute hackers, etc).
- Review and provide opinions on policies and Program documents such as Risk Assessments.

H. Chief, Administrative Services Bureau:

The Administrative Services Bureau shall be responsible for:

- Facilitating the coordination and review and process of DMAVA PSPs.
- Administrative maintenance of all Information Security PSPs applicable to DMAVA.
- Appropriate dissemination and posting of all DMAVA Information Security PSPs.
- Coordinating the review and approval process at the department and/or state level for all Information Security PSPs recommended by the Chief Information Officer for department-wide (Enterprise) adoption.

I. DMAVA Employees

All DMAVA employees and non-employees given access to DMAVA information and information resources shall:

- Sign a Statement of Understanding and follow DMAVA and unit-unique Information Security Policies, Standards, and Procedures.
- Report actual, potential, or suspected PSP infractions and/or security breaches to their immediate supervisor or the CISO.
- Attend training sessions for which they are scheduled
- All employees are required to promptly notify their immediate superior, should they detect any violation of these directives or any systemic weakness that needs correction. Supervisors should evaluate any such reports, document as necessary and interface with technical staff, or higher authority, to institute corrective action if warranted.

The proponent of this Directive is the Information and Administrative Servic
Division Users shall submit comments and suggested improvements directly
NJDMAVA, ATTN: Director, IASD, P.O. Box 340, Trenton, NJ 08625-034

OFFICIAL:

GLENN K. RIETH
Major General, NJARNG
The Adjutant General

DAVID S. SNEDEKER
Chief Information Officer
Acting Director, Information and Administrative
Services Division

DISTRIBUTION: A, A1, A2, B, C, D, E, F