PROJECTED COSTS RELATED TO BREACH

Vendor	Purpose	Projected Cost Covered Under Loan	Projected Cost Not Covered Under Loan	Paid to Date	To be Incurred	Totals
SourceLink	Stakeholder Outreach	$ 1,300,000		$ 1,020,000	$ 280,000	$ 1,300,000
DOR In-house Printing	Stakeholder Outreach		$ 936	$ 936		$ 936
Experian	Credit Monitoring	$ 12,000,000		$ 12,000,000		$ 12,000,000
Nelson Mullins	Legal Services	$ 300,000			$ 300,000	$ 300,000
Chernoff Newman	Breach Remediation	$ 200,000			$ 200,000	$ 200,000
LexisNexis	Breach Remediation	$ 20,000			$ 20,000	$ 20,000
Mandiant	Breach Remediation	$ 750,000		$ 738,692	$ 11,308	$ 750,000
	TOTAL BREACH COSTS	**$ 14,570,000**	**$ 936**	**$ 13,759,628**	**$ 811,308**	**$ 14,570,936**

PROJECTED COSTS RELATED TO SECURITY MEASURES

Vendor	Purpose	Projected Cost Covered Under Loan	Projected Cost Not Covered Under Loan	Paid to Date	To be Incurred	Totals
DOR	Structural Mgt Change & Personnel Additions		$ 174,138		$ 174,138	$ 174,138
DSIT	Two-Factor Authentication	$ 37,000			$ 37,000	$ 37,000
EMC	Encryption	$ 3,772,845			$ 3,772,844	$ 3,772,845
EMC	Disaster Recovery		$ 1,224,948		$ 1,224,948	$ 1,224,948
Miscellaneous Vendors	Network Segmentation	$ 690,000			$ 690,000	$ 690,000
Mandiant	System Monitoring		$ 90,000		$ 90,000	$ 90,000
Secunia	Patch Management	$ 42,000			$ 42,000	$ 42,000
TBD	Full-Disk (Workstation) Encryption	$ 25,000			$ 25,000	$ 25,000
TBD	DHCP	$ 50,000			$ 50,000	$ 50,000
Barracuda	Web Filter	$ 31,955			$ 31,955	$ 31,955
Solar Winds Lan Surveyor	Enhanced Logging and Monitoring	$ 6,000			$ 6,000	$ 6,000
TBD	Data Loss Prevention	$ 60,000			$ 60,000	$ 60,000
TBD	Windows Event Log Size/Scope Enhancements	$ 100,000			$ 100,000	$ 100,000
Cyber Ark	One-Time Password Management	$ 150,000			$ 150,000	$ 150,000
TBD	Intrusion Protection System	$ 200,000			$ 200,000	$ 200,000
Outside Consultants	Meeting the Recommendations of Outside Consultants	$ 435,200		$ 2,344	$ 432,856	$ 435,200
	TOTAL SECURITY COSTS	**$ 5,600,000**	**$ 1,489,086**	**$ 2,344**	**$ 7,086,741**	**$ 7,089,086**
TOTAL PROJECTED COSTS		**$ 20,170,000**	**$ 1,490,022**	**$ 13,761,972**	**$ 7,898,049**	**$ 21,660,022**

NOTE: *Existing resources are being reallocated to cover the cost associated with managing and implementing the above listed line items which do not include employee time.*

Senate Hearing 1-22-2013/ Reasons for Developing an Enterprise Security Program (See Fn 1)

A well-accepted definition of *enterprise governance* states:

> *Enterprise governance is the set of responsibilities and practices exercised by executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and ensuring that the organization's resources are used responsibly.*

Although many security professionals have encouraged management to take a more active role, many still do not understand that security requires action at the governance level. Based on the Agency's growing dependence on IT and IT-based controls, information and IT security risks increasingly contribute to operations and reputational risk. Management must understand the legal, technical, managerial, and operational considerations that converge in an enterprise security program. Treating adequate security as a **non-negotiable** requirement of the agency's responsibilities is critical.

Senior Management needs to thoroughly understand effective enterprise security governance and how to bring it about. For instance, beyond comprehending organizational structure, roles, and responsibilities, leaders need to understand the more detailed responsibilities and tasks required to develop and operate a sustainable security program.

Challenges to Consider:

- Appreciating the enterprise-wide nature of the security problem,
- Establishing the proper organizational structure and segregation of duties,
- Assessing security risks and the magnitude of harm to the organization,
- Determining and justifying appropriate levels of resources and investment,

In many instances, management does not understand the globally connected nature of the internet and how this facilitates access to information distributed throughout the DOR and its partners and customer base. Risks and opportunities increasingly derive from who you are connected to (your systems and networks) and who is connected to you. Borders, assuming they exist at all, have been greatly extended whether intended or not.

Governance and management of security are most effective when they are systemically woven into the very culture and fabric of the DOR's behaviors and actions. Effective security should be thought of as an attribute or characteristic of an organization. It becomes evident when everyone proactively carries out their roles and responsibilities, creating a culture of security that displaces ignorance and apathy. Elevating security to a governance-level concern fosters

attentive, security-conscious leaders who are better positioned to protect the DOR's **digital assets**, **operations**, and **reputation.**

Senior leadership's fundamental ***commitment*** to information security is the most important aspect of effectively managing the security risk for the DOR's digital assets. This requires internalizing security as an essential mission need, equivalent to core operational functions.

Enterprise security governance activities flow from the **fiduciary duty of care** owed by management to:

- Govern the operations of the organization and protect its critical assets,
- Govern the conduct of employees,
- Protect the reputation of the organization, and
- Ensure compliance requirements are met.

DOR will come to recognize that corporate governance is not just a matter of regulatory compliance and accountability, but a strategic means to lower the cost of operations, reduce risk, create value, and strengthen the long-term performance of the organization.

If the responsibility for the enterprise security is assigned to roles that lack the authority, accountability, and resources to implement and enforce it – and which do not have organization connection points horizontally and vertically throughout the organization the desired level of security will not be articulated, achieved, or sustained.

Contrary to the popular belief that security is a technical issue, even the best efforts to buy software-based security solutions and build security into developed software and operational systems encounter *"considerable resistance because the problem is mostly organizational and cultural, not technical.* " Effective security in today's interconnected environment requires integrating legal, managerial, operational, and technical considerations.

This shift in perspective elevates security from a standalone technical concern to an enterprise issue. Because security is now a business problem, the organization must activate, coordinate, deploy, and direct many of its core resources and competencies so security risks are managed and aligned with the entity's strategic goals, operational criteria, compliance requirements, and technical system architecture. To sustain enterprise security, the organization must move toward a security management process that is strategic, systematic, and repeatable, with efficient use of resources and effective, consistent achievement of goals - **such a process needs to account for the fact that policies, procedures, and technologies are dynamic.**

Following are three (3) characteristics of effective security governance:

Risk-Based
Security is considered as a cost of doing business and an investment rather than an expense or a discretionary budget-line item. Determining how much security is enough is based upon the risk exposure DOR is willing to tolerate, including compliance and liability risks, operational disruptions, reputational harm, and financial loss. Where impacts cannot be tolerated (disclosure of taxpayer information, for example), the threshold or tolerance is low and mitigation is required regardless of cost.

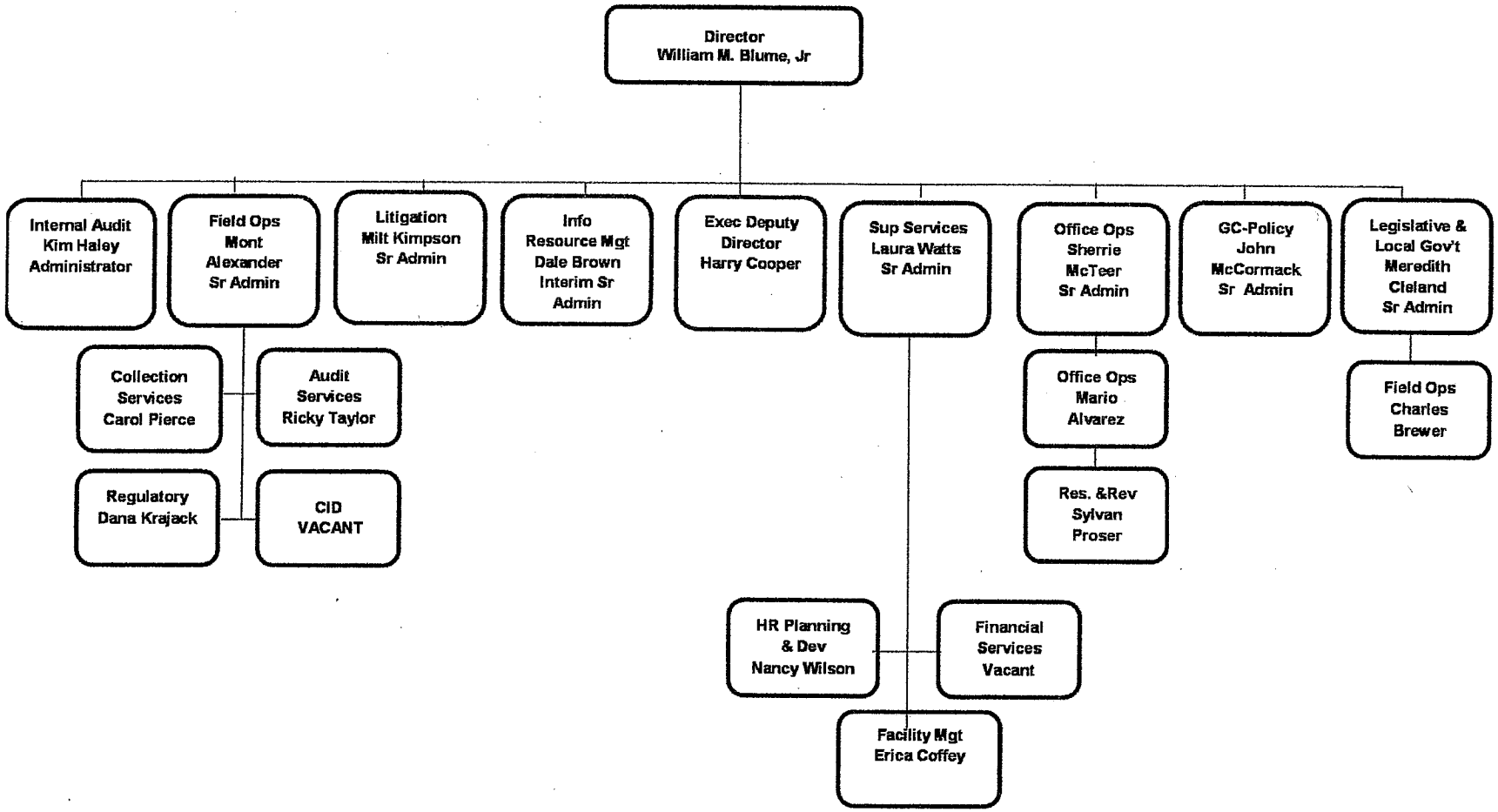
Addressed and Enforced in Policy
Security requirements are implemented through well-articulated policies and procedures. Rewards, recognition, and consequences with respect to security policy compliance are consistently applied and reinforced.

Cost / Benefit Not Easily Quantifiable
The effects of security are often intangible and addressing security at the enterprise-level is often hard to justify. Actions taken to securitize an organization's assets and processes are typically viewed as **disaster-preventing rather than payoff-producing** which make it difficult to determine how best to justify investing in security, and to what level. The benefits of security investments are often seen only in events that do not happen. As it is impossible to prove a negative, what value does an organization place on cost avoidance?

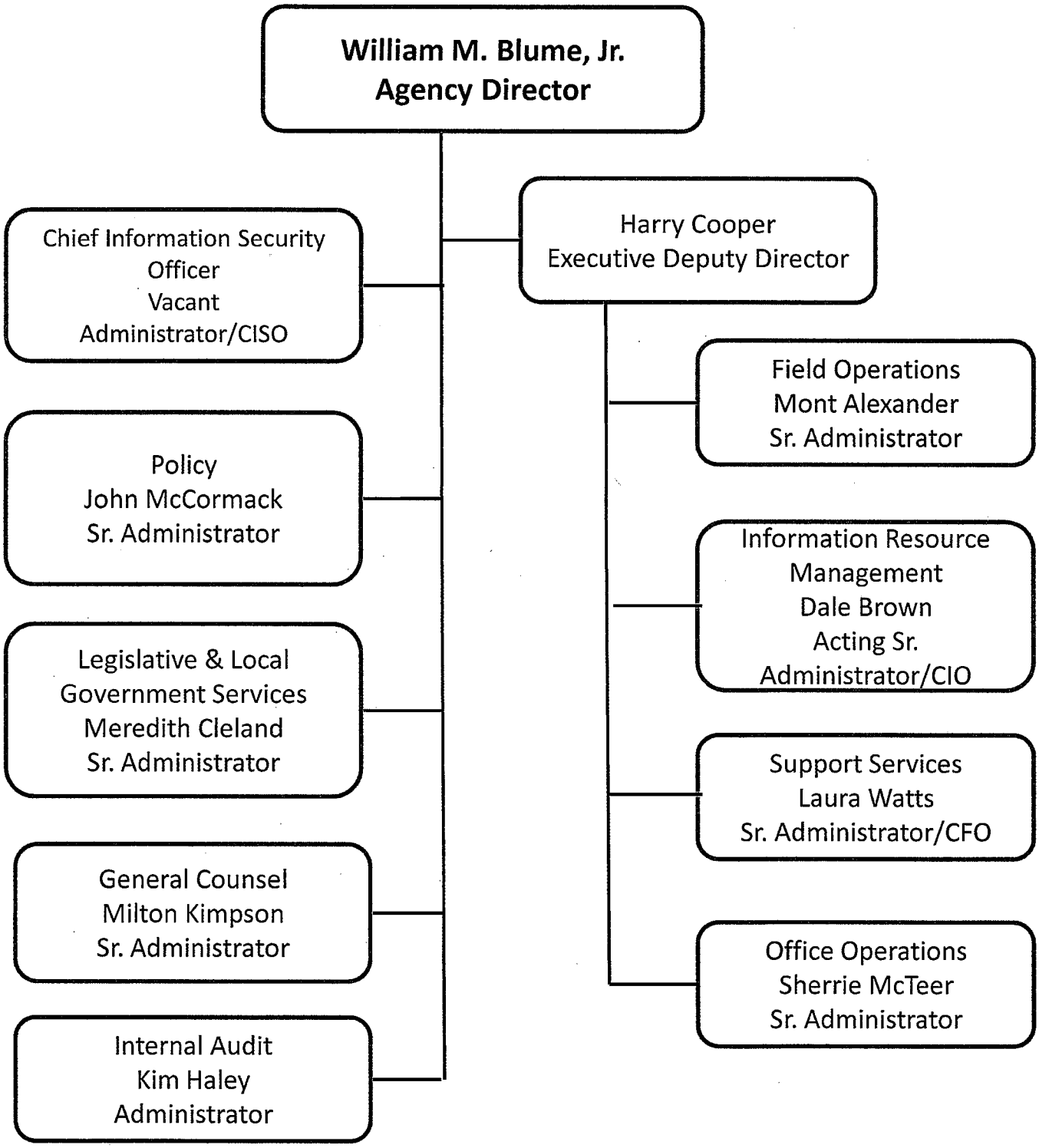
Many organizations do not approach security by deploying sound, commonly accepted practices; rather, they fix problems as they occur. As a result, establishing an enterprise solution can be an especially daunting task. Security is not a one-time project with a beginning and an end; it is an ongoing process. It requires continuous improvement, monitoring, measuring, and executing.

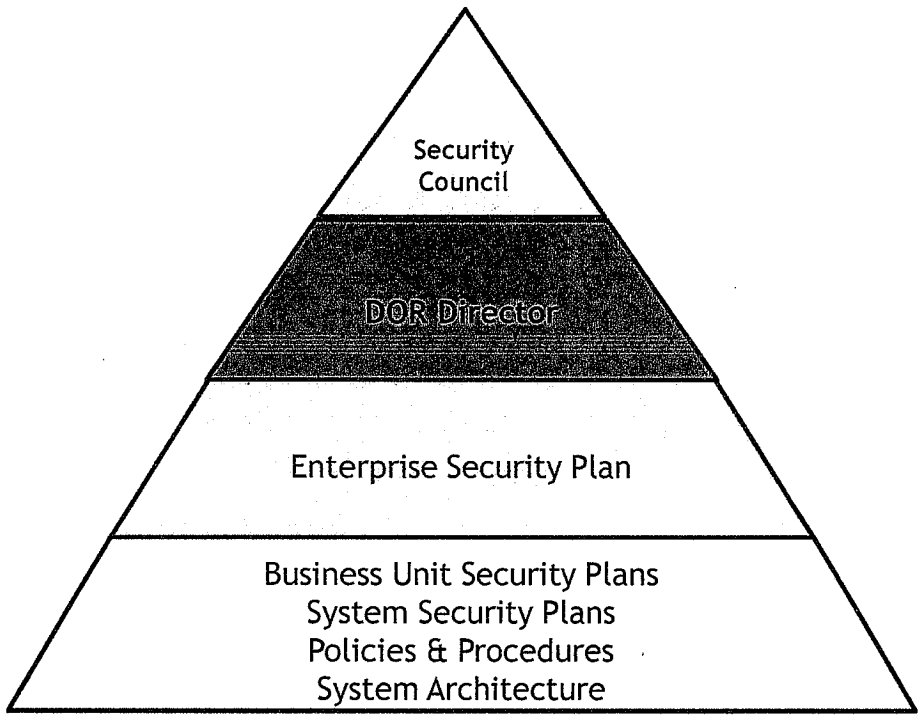
Governing for enterprise security means viewing adequate security as a non-negotiable requirement of DOR who is entrusted with taxpayer information. If DOR's management does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved, or sustained. To achieve a sustainable capability, DOR must make enterprise security the responsibility of leaders at a **governance-level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance.**

[1] All information included in this document is attributable to the following:
Governing for Enterprise Security (GES) Implementation Guide
Jody R. Westby, CEO, Global Cyber Risk LLC
Adjunct Distinguished Fellow, Carnegie Mellon CyLab
Julia H. Allen
Carnegie Mellon University, Software Engineering Institute, CERT®
August 2007


Director
William M. Blume, Jr
Internal Audit
Kim Haley
Administrator
Field Ops
Mont
Alexander
Sr Admin
Litigation
Milt Kimpson
Sr Admin
Info
Resource Mgt
Dale Brown
Interim Sr
Admin
Exec Deputy
Director
Harry Cooper
Sup Services
Laura Watts
Sr Admin
Office Ops
Sherrie
McTeer
Sr Admin
GC-Policy
John
McCormack
Sr Admin
Legislative &
Local Gov't
Meredith
Cleland
Sr Admin
Collection
Services
Carol Pierce
Audit
Services
Ricky Taylor
Regulatory
Dana Krajack
CID
VACANT
Office Ops
Mario
Alvarez
Res. &Rev
Sylvan
Proser
Field Ops
Charles
Brewer
HR Planning
& Dev
Nancy Wilson
Financial
Services
Vacant
Facility Mgt
Erica Coffey

SCDOR Organizational Chart, as of January 8, 2013





SECURITY COUNCIL

- The DOR Security Council will be made-up of the following:
  - DOR Director
  - Executive Deputy Director
  - Internal Auditor
  - Chief Information Security Officer (CISO)
  - Chief Information Officer (CIO)
  - General Counsel
  - Division of State Information & Technology (DSIT) Representative
  - Other internal and external parties on an ad-hoc basis as needed

- The Security Council is responsible for the coordination of security issues and the development and implementation of the Enterprise Security Plan (ESP).

- The team meets no less than monthly to discuss the effectiveness of DOR's security program and any new issues, and to coordinate and resolve problems.