Enterprise Cyber Security Architecture - Technical Approach

Cross Industry Solutions (CIS) Inc. provides business management & technology consulting in defining, designing & implementing innovative enterprise information and cyber security solution architectures across various industries and business domains for customer's strategic, mission oriented & highly visible programs such as setting up of Enterprise Center of Excellence (CoE) & Enterprise IT Modernization Plans/Blue Prints.

CIS delivers innovative business solutions with enabling state-of-the-art & leading-edge enabling technologies in compliance with Information Technology Assurance Framework (ITAF), Information Technology Security Standards (ITSS), Information Technology General Controls aligned in conjunction with National Institute of Standards and Technology (NIST) 800-53 Security and Privacy Controls, Capital Planning and Investment Control (CPIC), Federal Information Processing Standards (FIPS) Publications and Circulars, Federal Information System Controls Audit Manual (FISCAM), Federal Information Security Management Act (FISMA), The Center for Internet Security (CIS) Critical Security Controls (CSC) for Effective Cyber Defense and industry specific standards and frameworks and industry specific standards and frameworks like the Health Insurance Portability and Accountability Act (HIPAA), 'Corporate and Auditing Accountability and Responsibility Act' Sarbanes–Oxley (SoX), American Recovery and Reinvestment Act (ARRA), General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA) and various government laws & statutory regulations plus executive orders/circulars using various 3rd party Commercial off-the-shelf (COTS) & Government off-the-shelf (GOTS) products.

CIS SME's have knowledge, skills, leadership, bench strength and CIS financial stability of a large company with the agility and the customer-service focused responsiveness of a small business. CIS delivers the right combination of operationally proven process improvements using repeatable Capability Maturity Model Integration (CMMI) Level 3-5 model; Lean Six-Sigma (LSS) Black Belt certified resources; implementation of Information Technology Infrastructure Library (ITIL); Agile program/project management approach using Primavera P6, Project Management Body of Knowledge (PMBOK) Guide of Project Management Institute (PMI); Earned Value Management (EVM); Program Evaluation & Review Techniques (PERT) / Critical Path Methods (CPM) based tools & mechanisms for measuring project performance and progress; Financial Analysis using Government Finance Best Practices to leverage Generally Accepted Accounting Principles (GAAP); Project investment management lifecycle cost depreciation schedules consistent with Governmental Accounting Standards Board (GASB) with in-depth mission insight to meet our customer's goals and objectives.

Overview

Cross Industry Solutions (CIS) Inc. being in business for more than 22+ years solving many industry challenges with innovation has pioneered the next generation cybersecurity platform. This revolutionary platform will protect any enterprise sensitive, secret, and classified information and/or hacking of connected Internet of Things (IoT) devices, sacrificing of individual's private & personal information (PPI), from the unprecedented level of cyber intrusions and disruptions that has plagued governments, corporations, industries and everyday people all over the world for many decades.

FBI: Cybercrime losses tripled over the last 5 years.

Cybersecurity Ventures Official Annual Cybercrime Report. PHOTO: Cybercrime Magazine.

Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021

FBI: $3.5B Lost to Cybercrime in 2019, Led by Business Email Compromise

Cybercriminals are rapidly improving the sophistication of their attacks. The FBI estimates $3.5 billion was lost to cybercriminals last year; business email compromise caused the most damage.

- *Cybercriminals earned $1.5 trillion in 2018*
- *Cryptocurrency losses $4.5 billion in 2019*
- *Social media attacks cost $3.25+ billion per year*
- *Personal Data contributes $630 million per year*
- *The average data breach costs $3.92 million*
- *Cryptocurrency crime will increase 70% by 2021*
- *Cloud Data will increase 100x by 2021*
- *Internet users will reach 6 billions by 2022*
- *Global IoT devices market to 318 billion by 2023*
- *Cybercrime will increase nearly 70% by 2024*

Cybercrime Is World's Biggest Criminal Growth Industry

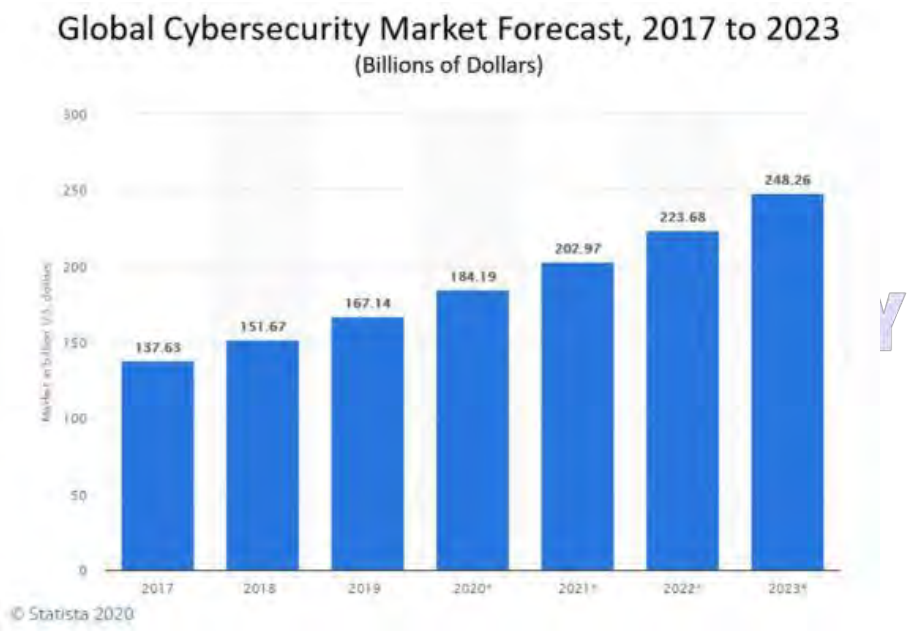
CIS's proprietary cybersecurity platform, "Cyber Geofencing" is an innovative, state-of-the-art, adaptable, trustable & end-to-end multilayer Integrated cybersecurity solution designed with a Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Cloud as a Service (CaaS)" and/or Software as a Service (SaaS) to address current Infrastructure & underlying technology limitations that failed to stop cybercrime, cyber-attacks and cyberterrorism.

Cybersecurity Investment – Market Size & Growth Opportunities

The cybersecurity market is segmented by solution into Identity and Access Management (IAM), risk and compliance management, encryption, Data Loss Prevention (DLP), Unified Threat Management (UTM), firewall, antivirus/antimalware, Intrusion Detection System/Intrusion Prevention System (IDS/IPS), security and vulnerability management, disaster recovery,

Distributed Denial of Service (DDoS) mitigation, web filtering, and others (application whitelisting and patch management).

According to a research report "Cybersecurity Market by Solution (IAM, Encryption, UTM, Antivirus/Antimalware, Firewall, IDS/IPS, Disaster Recovery, and DDOS Mitigation), Service, Security Type, Deployment Mode, Organization Size, Industry Vertical, and Region - Global Forecast to 2023", published by MarketsandMarkets, the cybersecurity market is expected to grow to USD 248.3 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 10% during 2018–2023. The major forces driving the cybersecurity market growth are strict data protection directives and rising cyber terrorism.



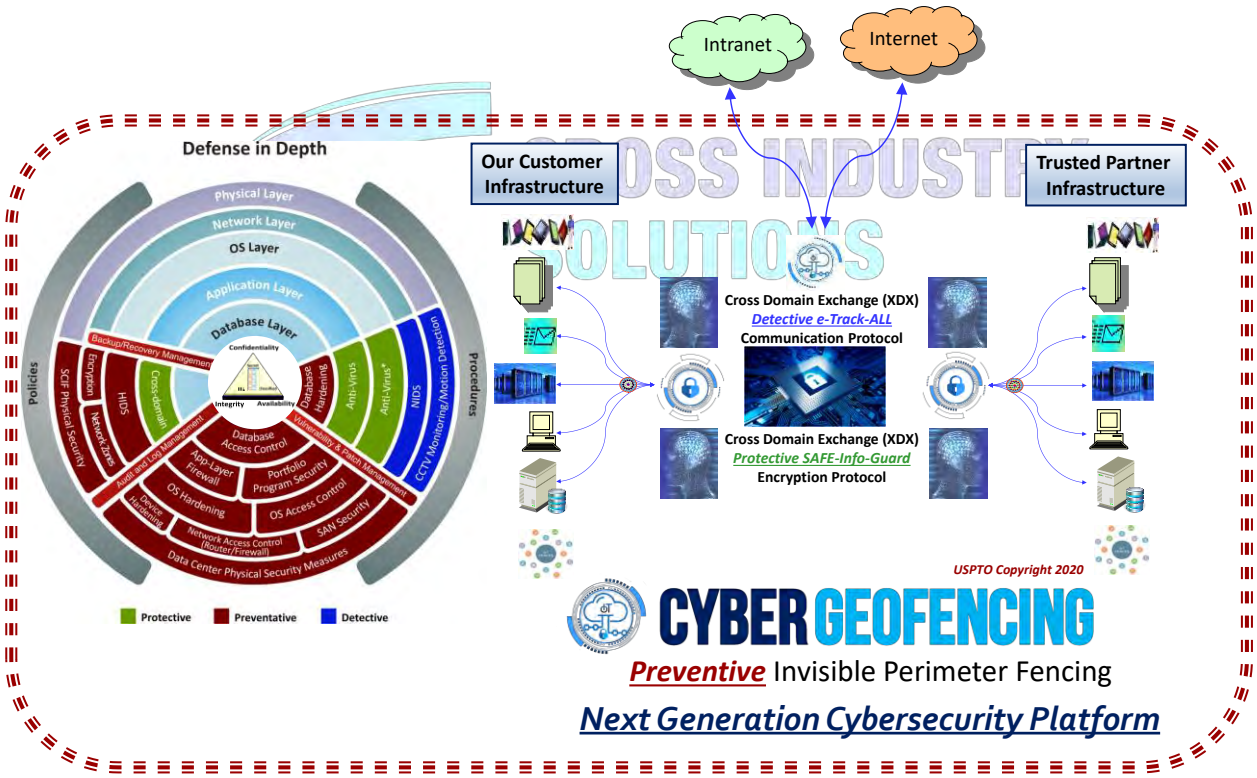
The global cybersecurity market will be worth $300B by 2024, according to Global Insights.

Integrated Cyber-Geofencing Solution

Our next generation innovative Geofencing platform is an **Integrated Cybersecurity Solution** as highlighted below that is designed to protect digital information assets, connected Internet of Things (IoT) devices and cross platform / cross domain communication across all infrastructure layers from eminent cyber-attacks by shielding all digital information assets/devices using

- ✓ "**Defense-In-Depth**" mechanisms in compliance with enterprise security policies, processes & procedures and statutory laws & regulations, mandates, executive orders and across all OSI layers over global communication grid
- ✓ **Cross Domain Exchange (XDX)** multifaceted platform independent architecture

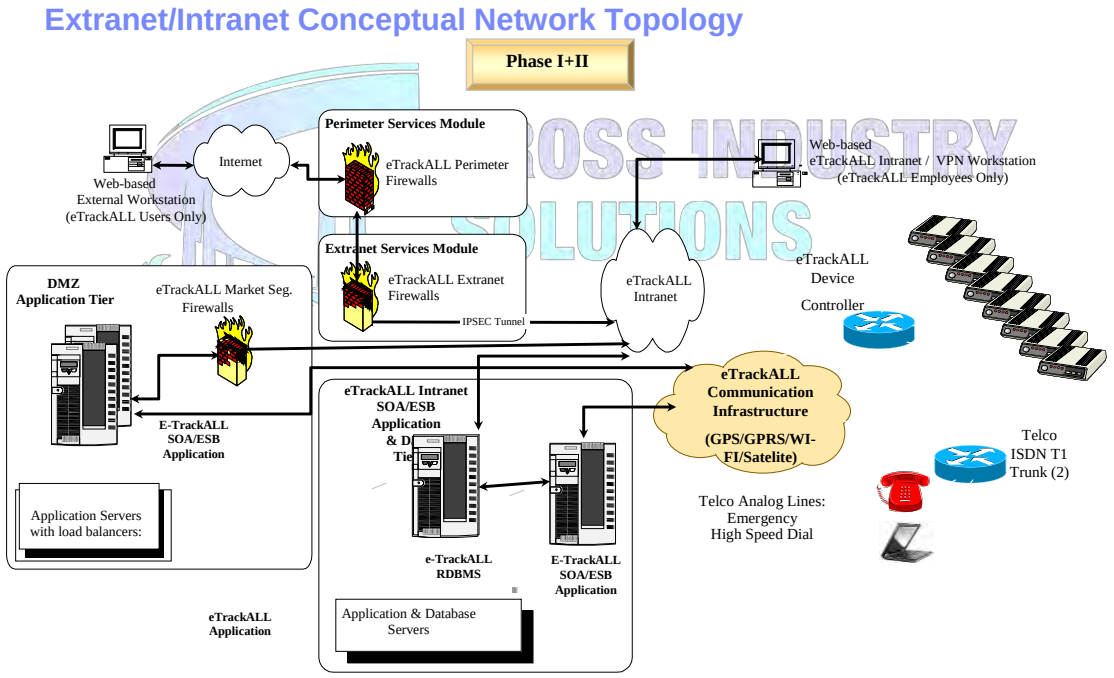
- ✓ A combination of Hardware (HW)/Software (SW) protocols with open & flexible PaaS/IaaS/CaaS/SaaS managed over a global **Geofencing Communication Grid (GCG)**
- ✓ Proprietary "**Preventive Cyber-Geofencing" that** acts as an invisible perimeter fencing to shield the identity of connected Internet of Things (IoT) devices
- ✓ **"Detective e-Track-ALL"** product for **e**lectronically **Track**ing of **All** digital information assets/devices and continuous monitoring & controlling of suspicious/fraudulent activities with Semantic & Artificial Intelligence (SI & AI) Algorithms and Machine Learning (ML) Language Metadata Environment (MDE)
- ✓ Unique "**Protective SAFE-Info-Guard"** work as a self-destructing multi-million-bit encryption product as **S**ecured **A**ccess **for E**nterprise **Info**rmation & **Guard**ing protocols to make stolen information totally useless as opposed to current flawed encryption systems and methods.
- ✓ Non-intrusive, most efficient & timely implementation



e-Track-ALL Continuous Monitoring & Controlling Protocol

The purpose of the electronic Tracking of All digital information assets and Intranet/Internet connected Internet of Things (IoT) devices at ALL the time across the globe is to provide the robust, highly scalable, open industry standards, flexible platform and communication framework that focuses on the most efficient and economical way, smart & intelligent detection of the least costly available GPS, GPRS, WI-FI or Satellite communication network using its state of the art innovative Ultra-Wideband Frequency Technology (UWFT) managed under Global Information Communication Grid (GICG) infrastructure. The e-Track-ALL protocol is also designed for continuous monitoring & controlling of suspicious/fraudulent activities with Semantic & Artificial Intelligence (SI & AI) Algorithms and Machine Learning (ML) Language Metadata Environment (MDE) empowered by Automatic Metadata Population Service (AMPS) for all registered digital information assets and IoT devices.

Following diagram highlights conceptual network topology for end-to-end operation of e-Track-All communication protocol over extranet Public internet and Private Intranet.



SAFE-Info-Guard - Self-Destructing Multi-Million Bit Data Encryption Protocol

When encrypting, the data has to remain secure and non-extractable even if one or more protection vectors are compromised. For this reason, CIS provides multiple levels of protection for the data. It is also critical that the CIS' unique encryption structure and methodology is kept highly confidential to challenge and discourage any potential cybercriminals from successfully accessing legible data. For this reason, not all details will be included.

While we cannot speak for all other encryption systems, we have included a list of faults and potential areas of vulnerability in current encryption systems such as:

- ✓ Include decryption keys in plain text.
- ✓ Use simple levels of encryption.
- ✓ Use the same encryption key for all areas.
- ✓ Fail to encrypt the network transport layer.
- ✓ Keep the full encryption keys in one location.
- ✓ Compromising one vector (e.g. the database server) causes all data able to be decrypted.
- ✓ Use of non-standard or easily broken encryption standards.
- ✓ Decryption keys use only letters, numbers or same-case.
- ✓ Short encryption keys.
- ✓ Missing an overall encryption layer.
- ✓ Missing salted passwords and random data.
- ✓ Plain text file and folder names help show what type of data is contained.

SAFE-Info-Guard Unique Differentiator

Following is the list of some of the key and unique differentiator between our multi-million-bit encryption protocol vs traditional 256-bit and/or pubic key infrastructure (PKI) that is being widely used:

- ✓ Self-destructing encryption product
- ✓ Multiple different encryption keys are used to access the different field data.
- ✓ All network traffic is AES 256 encrypted.
- ✓ The data file data is encrypted with multi-million-bits of key data.
- ✓ Standard AES 256 encryption is used with random levels of looping.
- ✓ Decryption key pieces are distributed amongst multiple cloud locations, compromising neither the server or the file data and will not render the data available.
- ✓ Decryption keys are randomly spliced, compromising both the server and the file data and will not render the data available.
- ✓ Decryption keys use different combinations of letters, numbers, cases and symbols.
- ✓ Decryption keys are usually very long and over 1,000 characters each.
- ✓ The file data is split into multiple parts and different random passwords are used for each part.
- ✓ The data file is encrypted with another overall level of AES 256 data protection.
- ✓ Random data is inserted into the encryption at varying points to lessen the chance of brute force decryption techniques.
- ✓ The file and folder names are entirely obfuscated and visible only within the application, stopping hackers from knowing which files or folders contain valuable or trivial data.
- ✓ All data is compressed before encrypting, not only to save space, but also to reduce the chance of finding binary patterns for matching common letters or words.

Approach to Perform and Manage the Work

CIS's cyber security management team is specialized in Enterprise Security Architecture (ESA) Management Program that supports our customer's mission and goals through engaging all stakeholders to design, build, and continuously improve effective and efficient security architecture, and within the context of their evolving strategic plans and goals.

In support of our customer's effort, CIS employs similar approaches and methodologies to those used to successfully support current and past HHS, DOJ and DHS/TSA & other high-profile enterprise security architecture projects across various industries including global government and commercial customers. Our other primary goal is to bring our best thinking – ESA subject area expertise, technical expertise, and open source community development and support – to ensure that our customers receives the best available technical and management support in achieving the vision for Enterprise Security Architecture. To this end, we have always provided highly qualified and appropriately experienced staff, and an approach to ESA task execution that leverages our corporate experience and the successful accomplishment of complex projects for other federal agencies and private sector customers for more than thirty years. Our technical approach addresses our customer's business requirements and aligns with their short and long-term strategic goals.

Knowledge of Industry Domains & Organization

CIS's Subject Matter Expertise (SME) has in-depth knowledge of various vertical and horizontal business domain integration knowledge with average of 30+ years of experience per resource. We understand our customer's strategic objective of the ESA Management & IT Services Program is to develop and maintain a secure, reliable, technically robust operating environment to support their mission goals and ensure accessibility and the highest data quality for the public.

The ESA IT Services Program provides the support that makes our customer's mission happen with a strong foundation. We also acknowledge our customer's mission is to create prosperity by strengthening the competitiveness of U.S. industry, promoting US trade and investment, and ensuring fair trade and compliance with trade laws and agreements. To achieve this mission and vision, CIS understands that our customer has laid out various goals such as:

1) advance U.S. international and commercial strategic interests;
2) enhance U.S. competitiveness in domestic and international markets;
3) broaden and deepen the U.S. exporter base;
4) identify and resolve unfair trade practices;
5) foster excellent relationships with customers and stakeholders; and
6) achieve organizational and management excellence.

Develop and Strengthen Customer's Enterprise Security Architecture (ESA)

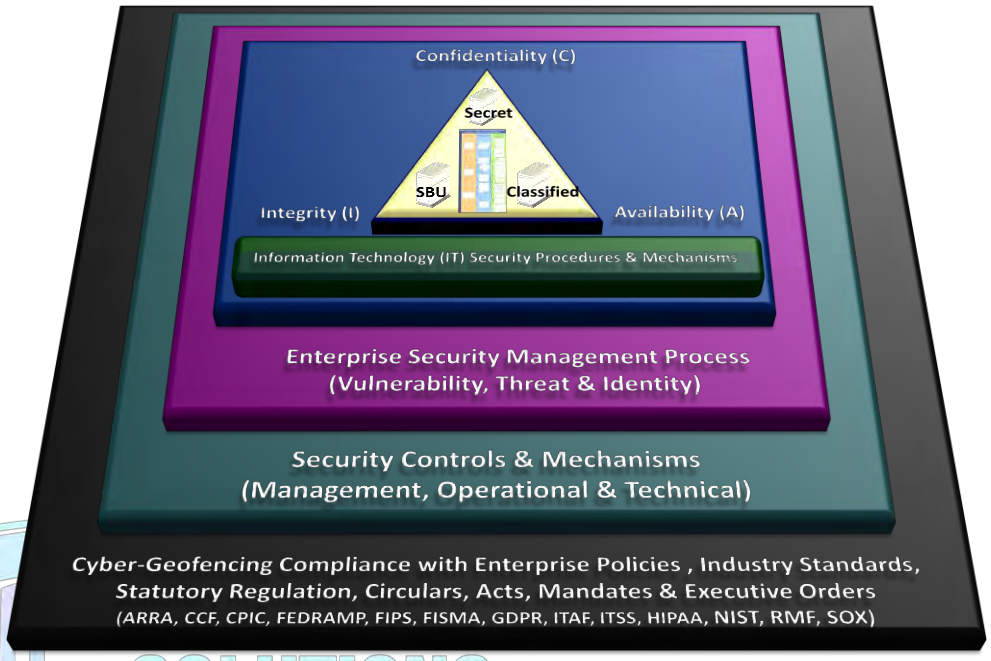
Our customer's ESA Program fulfills multiple Federal mandates related to planning and managing information technology (IT) investments and supporting organizational effectiveness. In addition, our customer's ESA Program ensures:

- ✓ The compliance with their Information Technology Assurance Framework (ITAF)
- ✓ Federal Risk and Authorization Management Program (FEDRAMP) Security Assessment Framework
- ✓ National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)
- ✓ Information Technology Security Standards (ITSS)
- ✓ Information Technology General Controls aligned in conjunction with NIST 800-53
- ✓ International Security Organization (ISO) 27001/27002 Security and Privacy Controls
- ✓ Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
- ✓ Capital Planning and Investment Control (CPIC)
- ✓ Federal Information Processing Standards (FIPS) Publications and Circulars
- ✓ Federal Information System Controls Audit Manual (FISCAM)
- ✓ Federal Information Security Management Act (FISMA)
- ✓ The Center for Internet Security (CIS) Critical Security Controls (CSC) for Effective Cyber Defense and industry specific standards and frameworks like:
  - The Health Insurance Portability and Accountability Act (HIPAA)
  - Corporate and Auditing Accountability and Responsibility Act' Sarbanes–Oxley (SoX)
  - American Recovery and Reinvestment Act (ARRA)
  - The General Data Protection Regulation (GDPR) 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area
  - Various government laws & statutory regulations plus executive orders/circulars using various 3rd party Commercial off-the-shelf (COTS) & Government off-the-shelf (GOTS) products.

All solutions and service developed for ESA program by CIS, meets our customer's Enterprise Security Architecture policies, standards, and procedures and developed according to customer Enterprise Security Plan.

CIS Cyber-Geofencing Security Architecture Framework & Model

CIS's Cyber-Geofencing Security Architecture Framework provides the holistic view of how security policies and standards map through various procedures and processes to implement the required security controls using numerous mechanisms. Our security architecture is a unifying framework of reusable mechanisms that implement policy, standards, and security risk management decisions. The security risk management, security policy and standards, and security architecture govern the security processes' in-depth architecture through design guidance, runtime support, and assurance mechanisms.



The above diagram summarized our top down view that will bridges the gaps while addressing Enterprise IT security from IT Security Standards (ITSS) and Policies to govern the implementation of security controls, security management processes, procedures and mechanisms to provide CIA (Confidentiality, Integrity and Availability) of Enterprise IT Services Portfolio Programs and Information at all time.

The Enterprise Operational Information Systems, like other IT systems in both the federal and private sectors, are potentially vulnerable to threats such as unauthorized access, destruction, disclosure, modification of data, and/or denial of service if the proper security controls are not identified and implemented. To mitigate potential threats and vulnerabilities to the Enterprise Information Systems, CIS have designed and implemented the information security architecture and provided privacy program support for highly visible programs within public and private sector industries. CIS provides the details of the framework that is required for implementing the appropriate security controls and mechanisms to protect the confidentiality, integrity, and availability of the Enterprise information and associated environments.

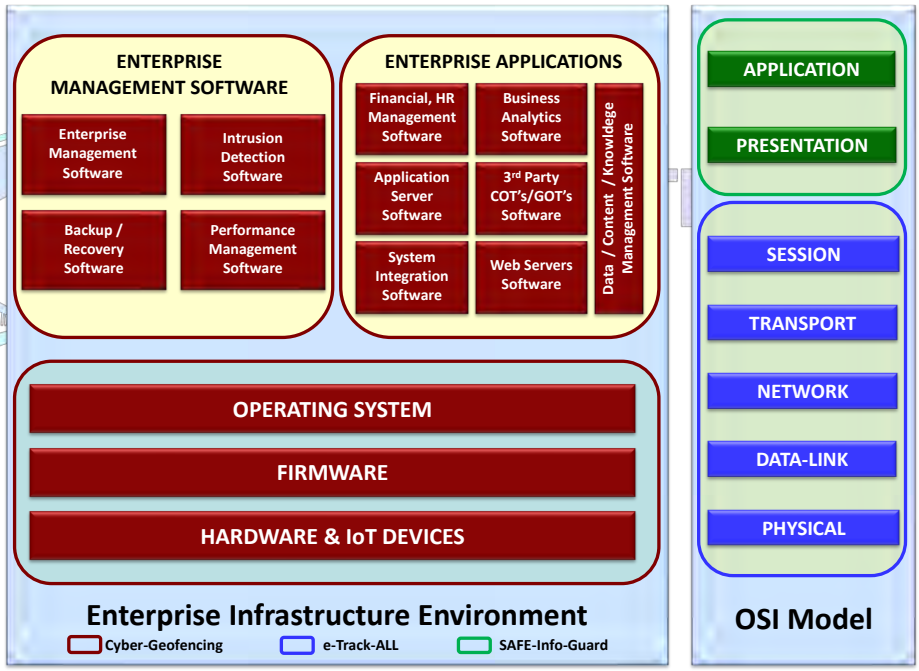
The Enterprise information will be guided by the following two overarching principles for the protection of information:

a) The Enterprise shall leverage existing security policies, processes, and mechanisms wherever possible. By applying existing federal/central and best industry standards, statutory laws, regulations and acts, IT security policies, processes, and mechanisms, the program benefits from their maturity and derives value from an existing investment.

b) The Enterprise shall apply defense-in-depth information security mechanisms. In doing so, the program effectively establishes multiple layers of controls to protect the confidentiality, integrity, and availability of Enterprise IT Services Portfolio Programs information that can fall under anyone or more security levels level like Secret, Classified and Sensitive but Unclassified (SBU) information.

Cyber-Geofencing Solution - Security Management Process

The security processes carry out the intent of the enterprise risk management, security policy and standards, and security architecture. They are broken into discrete data domains such Sensitive, Classified, Secrete, Sensitive but Unclassified as they solve very different problems, and require different staffing, support models, and success criteria.



CIS's Security Management Team (SMT) & Operational Support Staff (OSS) works closely with our customer's Chief Security Officer (CSO) in implementing various procedures, processes and controls as discussed below and our customers can leverage the subject matter expertise of CIS and enterprise security architecture that CIS have designed and implemented on various programs within public and private sector organizations using OSI model and within the system boundaries as highlighted in adjacent diagram. Following section highlights CIS's key security

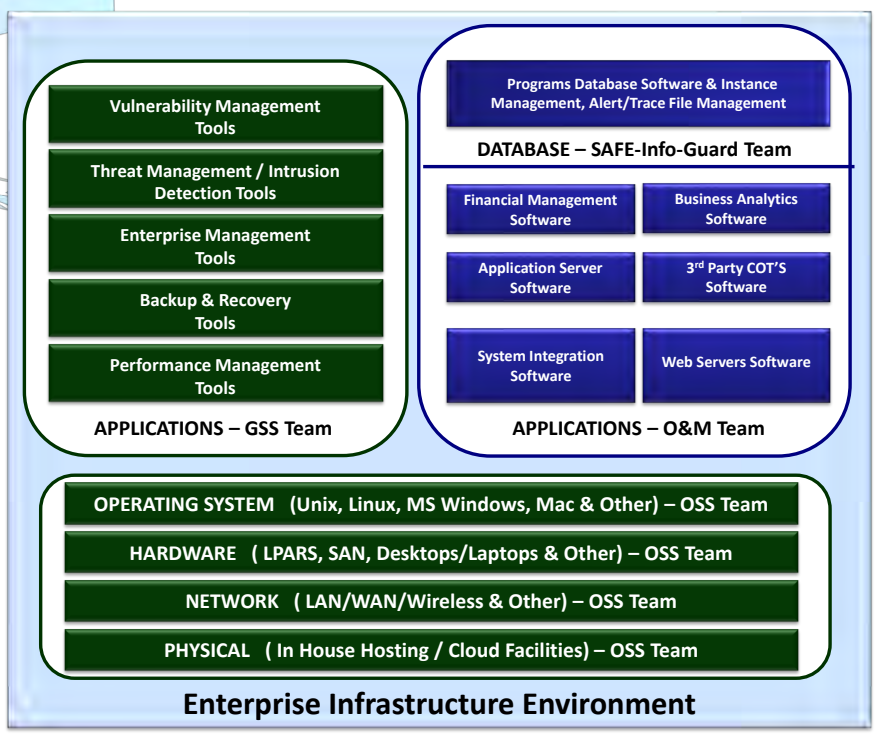
management processes that our customers need to consider in protecting IT service Portfolio Programs from security breaches and significant revenue losses due to security act violation and potential litigations. The enterprise information security implementation across physical, network, host and operating system, application and database layers shall be in compliance with the customer's IT Security Standards.

System Boundaries

The Cyber-Geofencing solution empowered by underlying e-Track-ALL and SAFE-Info-Guard protocols is designed to protect enterprise and individual digital information assets that is stored, managed and accessed by any IoT devices, applications and interfaces. The below diagram illustrates the Cyber-Geofencing and integrated e-Track-ALL and SAFE-Info-Guard protocols system boundaries for the enterprise infrastructure environment and with reference to Open Systems Interconnection (OSI) Seven Layer Reference Model.

Cyber-Geofencing - Enterprise Identity, Threat & Vulnerability Management

The enterprise **Identity management** within customer's system boundary shall be applicable to enterprise application and database level access, authentication and authorization mechanisms. The enterprise **threat management** shall deal with the threats to customer's systems such as virus, Trojans, worms, malicious hackers, and intentional and unintentional system misuse by insiders or outsiders. The threat management tools and processes were implemented by OSS and it resides outside customer system boundary. The enterprise **vulnerabilities** shall reside at network layer, host and operating system layer, application layer and database layer. The vulnerability management tools and processes shall be implemented by OSS and Customer SMT. Following Figure#5 highlights our conceptual view about the our customer's environment that will be supported and maintained by on-site General Support System (GSS) group and Operation & Maintenance (O&M) group.



Cyber-Geofencing Solution - Enterprise Security Implementation Roadmap

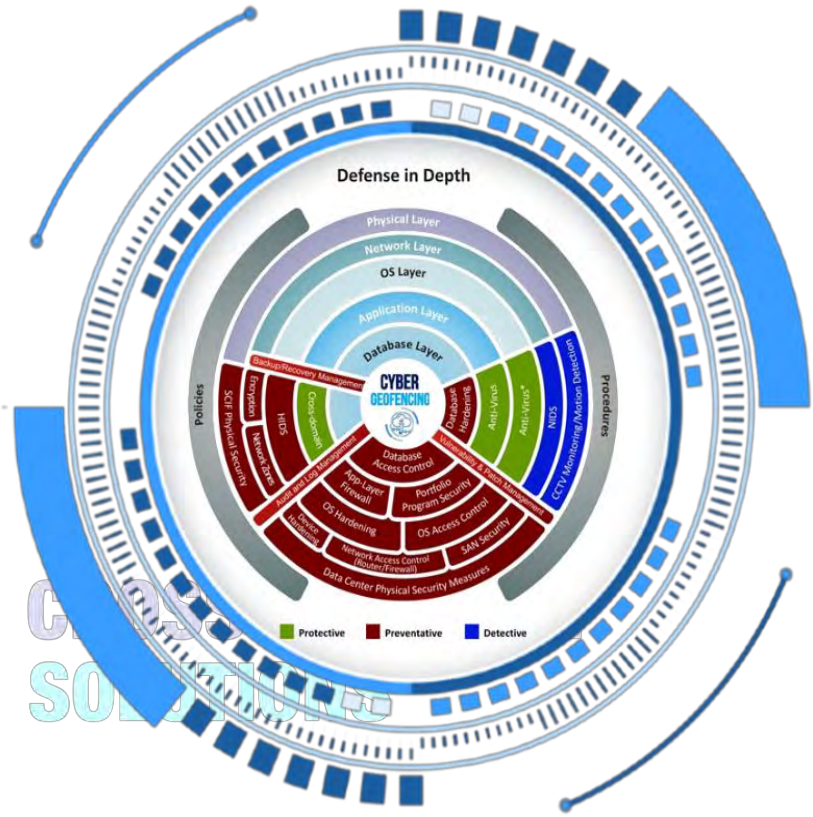
The enterprise IT security functions shall focus on the following three key elements of customer's system security requirements, architecture, design and deployment point of view:

- Protect enterprise information Confidentiality, Integrity & Availability point of view
  - ***'What' needs to be protected?***
- Enterprise information protection mechanism, procedures and processes
  - ***'How' it will be protected?***
- The responsible parties who manages ENTERPRISE information protection
  - ***'Who' is the responsible party?***

Above diagram highlights our proposed Cyber-Geofencing Enterprise Security Implementation Plan with what need to protected, how it can be protected and who are the responsible parties to implement recommended processes, policies, procedures and mechanisms.

Cyber-Geofencing - Enterprise Security Control (Defense in Depth)

Enterprise Defense in depth is predicated on the notion that every security control is vulnerable somehow, but that if one component fails another control at a separate layer still provides security services to mitigate the damage. Each level of the defense in depth stack has its own unique security capabilities and constraints. The core security services - authentication, authorization, and auditing apply at all levels of the defense in depth stack, for example audit logging occurs at network, host, application, and data access levels. The security architect is responsible to identify the proper combination of the core security services at each level in the stack to deliver a cohesive security posture that reflects the enterprise's risk management objectives. Following diagram highlights our vision about our customer's layered security and associated protective, preventive and detective mechanism and processes.



Enterprise Physical Security

Physical security is the operations for security mechanisms for the physical working locations, data and application hosting centers. Physical security mechanisms, such as physical access authorizations, physical access control, access control for transmission medium, access control for display medium, monitoring physical access, visitor control and access Logs.

Enterprise Network Security

Network security is the design and operations for security mechanisms for the network. Network security mechanisms, such as network firewalls and network intrusion detection devices (NIDS), are generally a convenient and scalable point to apply security controls and are an important

locale for defining chokepoints and zones. Zones define logical and/or physical boundaries around a group of systems, for example the DMZ pattern in web applications. Chokepoints define places to cross boundaries into and out of zones, where special security considerations apply.

Enterprise Host & Operating System Security

Host security is concerned with access control on the servers and workstations. Host Intrusion Detection Systems (HIDS) identify host anomalies and security events. Host Integrity Monitoring checks and protects the integrity of the critical files and programs on the host. Baseline Configuration Scanners provide assurance that the systems in use in the field meet the policy and standards at a granular level. These scanners may be automated to support highly distributed and large-scale environments. Using the zones and chokepoints defined in the network security architecture, the security architecture defines a baseline configuration for each locale.

Enterprise Application Security

Application security deals with two main concerns:

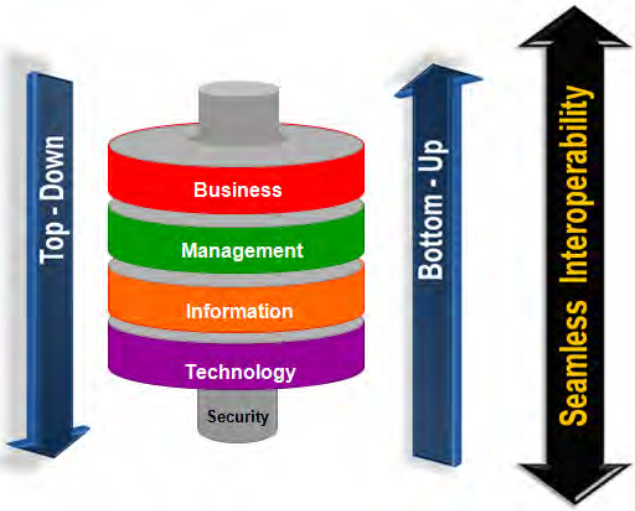
1. Protecting the code and services running on the system, who is connecting to them, and what is output from the programs through a combination of secure coding practices, static analysis, threat modeling, participation in the SDLC, application scanning, and fussing.
2. Delivering reusable application security services such as reusable authentication, authorization, and auditing services enabling developers to build security into their system. Security frequently collaborates with software architects and developers in this area to build security into the system.

Enterprise Data Security

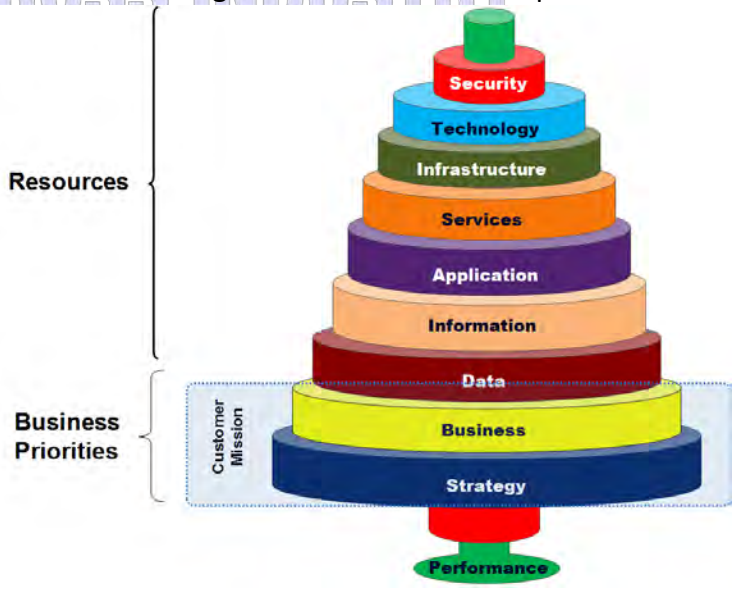
Data security deals with securing access to data and its use; this is a primary concern for the security architecture and works in concert with other domains. Vulnerability management tools conduct specialized scans against database hosts. The SDLC defines secure patterns for database integration based on data classification defined in the policy. Database intrusion detection and monitoring provides ongoing intelligence as to the threats against the database. The value in performing detection and monitoring at this layer is that attackers may not traverse the expected path to get to the asset that the security system is trying to protect: data. Database, XML documents, transient messages, and other resources are protected by data security mechanisms. Security frequently collaborates with database administrators in this area to drive secure database configuration and operations.

Enterprise Architecture (EA) Framework & Cross-Cutting Security Domain

CIS SME's have analyzed and completed unprecedented level of various clientele existing enterprise architecture and identified existing architecture components to determine what information need to be collected from their current environment by investigating, analyzing, with Top-down and Bottom-up approach with seamless interoperability across all EA domains and managing EA Program performance by leveraging innovative and open source integrated tools & technologies. Our Chief Architects and Security Architects work with our strategic teaming partners and customers CIO office, Strategic System Management Office (SSMO), Program Management Office (PMO), Sr. Executives Leadership and stakeholders, other team leads/authorities to design and recommend target architecture based on other federal/state government experience in deployment of such architectures for other departments. The target architecture included better integration with other enterprise tools.



We have completed numerous in-depth analysis and prepared Enterprise Architecture (EA) Framework that has been organized hierarchically into a baseline five-layer (Business, Management, Information, Technology and security) model and into a ten-layers (Strategy, Business, Data, Information, Application, Services, Infrastructure, Technology, Security and Performance) improved / recommended where the initial layers represent base levels of abstraction identifying business and strategic concerns, while subsequent higher layers focus on more detailed aspects of the architecture typically more technical or detailed in nature. In this way, the definition of customer's EA Framework follows the paradigm of other widely used EA frameworks such as the Zachman/TOGAF/DODAF Framework by incorporating levels of abstraction within the architecture. The Security and Performance components were also designed to be integrated into all layers of the customer's EA framework as cross cutting and overarching, given the importance of security as well as the performance in all components of the meta model.



Enterprise Security Policies & Standards

Our ESA SME's prepares the Information Technology Security Program Management Plan for our customer which is the foundational document that describes the Customer's approach to securing all systems. In addition, Customer's IT Security Policies, any statutory regulations, or its successor, and the associated IT Security Standards provide the minimum-security requirements that any Customer's IT system must follow. Our SME's incorporate IT Security Standards those are based on the security control categories listed in NIST Special Publication (SP) 800-53. Our customer's IT Security Standards outline policies are crafted to meet the controls listed in the NIST publication.

Our customer's IT Security Standards are divided into the three security control categories used by NIST: management, operational, and technical controls. Systems development, deployment, and operations are guided by a hierarchical set of policies. Federal laws, regulations, and executive mandates, along with high level customer's policies, that provide the overarching basis for many of the lower level standards and policies.

The hierarchy of our customer's IT Security Policies and IT Security Standards (ITSS) those were implemented and supported by Office of Chief Information Officer (OCIO) and customer's Operational Support Systems (OSS), Operation and Maintenance (O&M) staff and Security Management Team are listed in the following tables.

Table 1: Overarching Edicts

Overarching Edict	List
Federal laws, regulations, and executive mandates	Federal Information Security Management Act (FISMA), Federal Information System Controls Audit Manual (FISCAM), U.S. Section 552a - the Privacy Act, Public Law 100-235 - The Computer Security Act, National Institute of Standards Technology (NIST), 28 Code of Federal Regulations (CFR) Part 17, 32 CFR Part 200, DCID 6/3, 6/4, 6/9.
Customer Division/Department level	Executive Order (EO) 12958 - as amended, EO 12968, Technical Reference Manual (TRM), and Security Program Operating Manual (SPOM), HIPAA, SOX, CPIC, ARRA

Table 2: IT Security Standards

ITS Standard Identifier	ITS Standard Family	ITS Control
RA	Risk Assessment	Management
PL	Planning	Management
SA	System and Services Acquisition	Management
CA	Certification, Accreditation, and Security Assessments	Management
PS	Personnel Security	Operational
PE	Physical and Environmental Protection	Operational
CP	Contingency Planning	Operational
CM	Configuration Management	Operational
MA	Maintenance	Operational
SI	System and Information Integrity	Operational
MP	Media Protection	Operational

ITS Standard Identifier	ITS Standard Family	ITS Control
IR	Incident Response	Operational
AT	Awareness and Training	Operational
IA	Identification and Authentication	Technical
AC	Access Control	Technical
AU	Audit and Accountability	Technical
SC	Systems and Communication Protection	Technical

Table 3: OCIO/ITSS/OSS Security Policies and Standards

Security Domain	Policies/Standards
Information Risk Management	ITSS Risk Assessment ITSS System and Services Acquisition ITSS Planning ITSS Classified Laptop and Standalone Computers ITSS Awareness and Training
Business Continuity and Disaster Recovery	ITSS Contingency Planning OSS Contingency Space Assignment Policy OSS Emergency and Mission-Critical Emergency Employees Policy
Incident Response	ITSS Incident Response
Physical and Environmental Security	ITSS Personnel Security ITSS Physical and Environmental Protection OSS JDC Delivery Policy OSS JDC Property Pass Policy OSS JDC Parking Policy OCIO Personnel Security Administration Policy OSS Use of Small Cooking Appliances in Data Center Space Policy
Identity and Access Management	ITSS Identification and Authentication ITSS System and Information Integrity ITSS Access Controls ITSS Media Protection OSS Un-trusted Device Security Policy OSS Inactive User Accounts Policy OSS JDC Annual Physical Access Recertification Policy OSS JDC Door Key Management Policy OSS JDC Tour Policy OSS System Re-access Certification Policy
Systems Development Lifecycle	ITSS Maintenance ITSS System and Communication Protection ITSS Configuration Management OSS Change Management Policy OSS Media Handling, Disposal and Reuse Policy
Audit and Compliance	ITSS Certification, Accreditation, and Security Assessments ITSS Audit Accountability OSS Audit Trail Review Policy

The security architecture design presented by our SME's describes how the system is in compliance with our customer's IT Security Standards. Within given program/project, the various mechanisms required to protect program/project information from vulnerability across physical, network, operating system, application and database communication layers have been implemented.

The appropriate procedures implemented by our SME's will enable secure end-to-end communication between program/project end user/client desktop, middleware web and application servers and backend information storage servers that are within the scope of our customer's program/project architecture design. The target program/project, where feasible, has enhanced the minimum-security requirements in compliance with our customer's IT Security Standards to support secure transactions of program/project's business, delivery of information between department, Components and other federal, state and our customer's program/project business trading partner companies.

Enterprise Security Processes

Our proposed enterprise security processes are guided by the policies and standards listed in the previous section; several processes have been developed to enforce them. Additionally, we ensure that the customer's program/project has established other processes to protect information in support of the centralized services promulgated under the given program/project of Customer Service Level Agreement (CSLA). The information security processes have been categorized into seven information security domains and are listed in the following tables.

Table 4: Enterprise Security Processes

Security Domain	Processes	Performing Entity
Information Risk Management	Vulnerability and Patch Management	PMO, SMT, GSS, OSS
	Risk Assessments	GSS, OSS
	Privacy Impact Assessment	PMO, SMT
	Systems Security Plan	PMO, SMT
	Security Management Plan	PMO, SMT
Business Continuity and Disaster Recovery	Continuity of Operations Plan (COOP)	PMO, SMT, GSS, OSS
	Information Technology Contingency Plan (ITCP)	PMO, SMT, GSS, OSS
	Disaster Recovery Plan (DRP)	GSS, OSS
Incident Response	Incident Response Plan	PMO, SMT, GSS, OSS
Physical and Environmental Security	Personnel Security	PMO, SMT, GSS, OSS
	Physical and Environment Monitoring	GSS, OSS
Identity and Access Management	Application Access	GSS, O&M Team
	Database Access	GSS, O&M Team
	Network Access	OSS
	Operating System	SMT, OSS, O&M Team

Security Domain	Processes	Performing Entity
	Physical Access Control	PMO, SMT, OSS
Systems Development Lifecycle	Security Testing	PMO, SMT, GSS, OSS
	Change Management	GSS, OSS, O&M Team
	Quality Assurance (QA) and System Review	GSS, OSS, O&M Team
	Certification & Accreditation (C&A)	PMO, SMT, GSS, OSS
	Performance and Capacity planning	GSS, OSS, O&M Team
Audit and Compliance	Vulnerability and Patch Management	PMO, SMT, GSS, OSS
	FISMA, ITAF, FEDRAMP, CSF, CSA CCM, FIPS	PMO, SMT, GSS, OSS
	FISCAM, ISO 27002/27002, NIST 800-53 Audit	PMO, SMT, GSS, OSS

The security processes listed in the above table provides the confidentiality, integrity, and availability services for our customer's specific program/project platform. Security processes are implemented as protection services, such as authentication and authorization, detection services, such as monitoring and auditing, and response services, such as incident response and forensics.

Sample security processes for our customer's program/project are listed in Table 5 below, in relation to Security Layers, Mechanisms and Procedures.

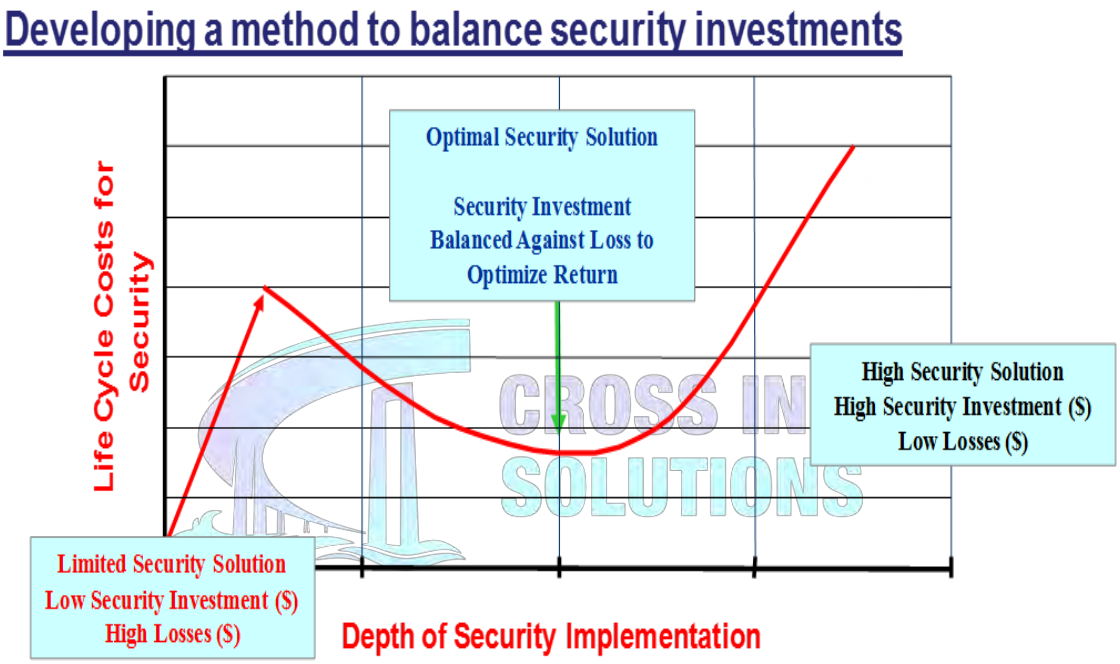
Table 5: Security Implementation Across Various Layers

Implementation Layer	*'WHAT'* Needs to be Protected? (Identity / Threat / Vulnerability Management)	*'HOW'* It will be Protected? (Tools / Mechanisms / Processes)	*'WHO' Is the Responsible Party?*
Physical	Unauthorized and Unauthenticated Access to the JDC-W or JDC-D	Visitor Logs Government Issued IDs Human Guards Access Control Badge Access Control Closed Circuit TV (CCTV) Motion Detectors Certification and Accreditation (C&A) Process	GSS, OSS, PMO, SMT

Implementation Layer	*'WHAT'* Needs to be Protected? (Identity / Threat / Vulnerability Management)	*'HOW'* It will be Protected? (Tools / Mechanisms / Processes)	*'WHO' Is the Responsible Party?*
Network	Unauthorized and Unauthenticated Access to Any Hardware and Software. Secure Internal and External Communication Secure Data and Information Access and Flow Secure Network Logs, Traces, Vulnerability Scan Logs and Reports	User Accounts - Network Device Access Access Control List (ACL) Firewall Rules DMZ Virtual Private Network (VPN) Virtual Local Area Network (VLAN) LAN /WAN Vulnerability Scans (operating system, SW, Open Ports for Protocols) NIDS	OSS, SMT
Host and Operating System	Unauthorized and Unauthenticated Access to Any Logical Partitions (LPARS). Secure Operating System, Application, Database and other source code, data files, and logs. Vulnerability Scan Reports Secure Application Journal Logs, Secure Database Journal Logs, Dumps (System, Core, and User).	User Accounts - LPARS Access Control List (ACL) File System / Directory Structure Protection File Protection Vulnerability Scan	OSS, SMT
Application	Unauthorized and Unauthenticated Access to Any Application System and Data	Application User Accounts Application Role Base Security Vulnerability Scan External Communication	GSS, SMT, O&M Team
Database	Unauthorized and Unauthenticated Access to Any Data	Database User Account Database System and User Privileges Database Roles Database Views Database Synonyms	GSS, SMT, O&M Team

Enterprise Security Investment

Our subject matter experts who were providing their expert opinion to the federal and commercial customers to justify the cost of security investment and the level of depth enterprise systems may need based on the overall business impact and Return on Investment (ROI). The diagram below provides guidance to our customer to meet their strategic priorities and goals to implement security with acceptable level of risks by optimal investment to reduce the revenue loss due to security breaches.



Goal: Invest to mitigate security risks

To: Reduce the dollars lost due to security breaches

While: Not over investing where there is no return on investment