Developing a Framework to Improve Critical Infrastructure Cybersecurity: An RFI Response

This RFI response is a collaborative effort between Alpha Terra Engineering, Inc. and Cybersalus, LLC. The principal authors of this RFI response are:

- Mr. Fred Waterman, P.E., CCM Principal Engineer/Vice President Alpha Terra Engineering, Inc.
- Brigadier General Thomas Verbeck, Ret, President of Cybersalus, LLC
- Mr. Dana Shafie, NSA-IAM, Executive Vice President of Cybersalus, LLC

Introduction

Alpha Terra Engineering, Inc. (ATEI) and Cybersalus LLC are pleased to respond to NIST's RFI. NIST has been tasked to develop a 'Cybersecurity Framework' consisting of "standards, methodologies, procedures, and processes to align policy, business, and technological approaches to address cyber risks" to our nation's critical infrastructure. The proposed Framework is intended to:

- Identify cross-sector security standards and guidelines applicable to critical infrastructure
- Increase visibility and adoption of those standards and guidelines
- Find potential gaps to be addressed through collaboration with industry and industry-led standards bodies
- Incorporate voluntary consensus standards and industry best practices and be consistent with voluntary international consensus-based standards
- Be compatible with existing regulatory authorities and regulations.

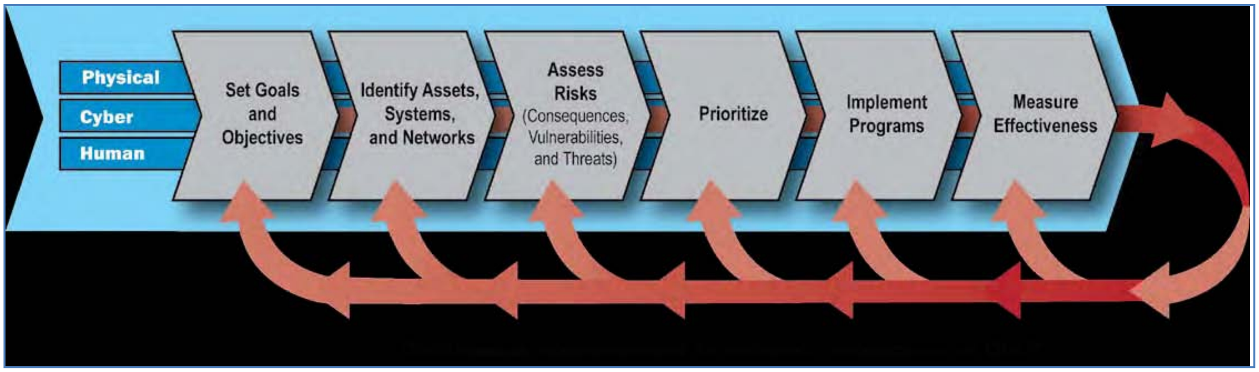
Presidential Policy Directive 21, Critical Infrastructure Security and Resiliency released in Feb 2013 "requires the federal Government work with critical infrastructure owners and operators and other Government entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure".

"All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions".

Our input to this RFI is written to address these two important goals through a discussion of the ***Foundational Concepts of Critical Infrastructure Protection*** and also the comprehensive ***evaluation of risk and risk-reduction options*** such as ***cyber risk insurance.*** The proper evaluation of risk, and consideration of the full spectrum of methods for mitigating this risk, is essential to constructing a lasting and useful Framework that can help Critical Infrastructure and other communities to cope with the continuously evolving threat.

Foundational CONCEPTS of Infrastructure Protection

The Nation's critical infrastructure consists of three realms—physical, cyber and human—functioning interdependently to provide the means and mechanisms by which critical services are delivered throughout our Society. These realms and how they interrelate are depicted in the graphic below. Because Government shares responsibility with Industry in the operation of our economy, protection of our system of commerce must be a shared responsibility. The Government's central role must be to help guide development of the overall Framework outlining the means, methods and measures to effectively protect the security of our critical infrastructure from threats of cyber attack.


Physical
Cyber
Human
Set Goals and Objectives
Identify Assets, Systems, and Networks
Assess Risks (Consequences, Vulnerabilities, and Threats)
Prioritize
Implement Programs
Measure Effectiveness

Infrastructure Protection Process, National Infrastructure Protection Plan (Source: DHS, NIPP)

The Framework must be developed in coordination and cooperation with the owners and operators who fully understand the detailed complexities of their infrastructure systems. Their knowledge and management controls are essential to attain a risk management preparedness addressing the full spectrum of threats and hazards. The nature of this crucial mission requires close collaboration with the appropriate Industry groups and state and local government in designing effective, adaptive risk mitigation strategies and incentives. The Framework must also be adaptable to an evolving risk environment, with flexibility to quickly accommodate risk information allowing stakeholder partners to develop and implement innovative defensive measures.

The President has directed that the Framework "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework".

The Executive Order recognizes that open public review and comment from the general Public, Sector-Specific Agencies, owners and operators of critical infrastructure, and key stakeholders is essential for successful planning and implementation. It is also essential to meet defined performance goals. Members of the Critical Infrastructure Partnership Advisory Council are provided here:
http://www.dhs.gov/council-members-critical-infrastructure-partnership-advisory-council

Critical infrastructure sectors and associated federal department Sector-Specific Agencies (SSAs) are designated by the Directive. DHS is responsible for evaluating changes to critical infrastructure sectors and to consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated SSA for that sector.

The 16 critical infrastructure sectors and SSAs follow, with key industry standards groups:

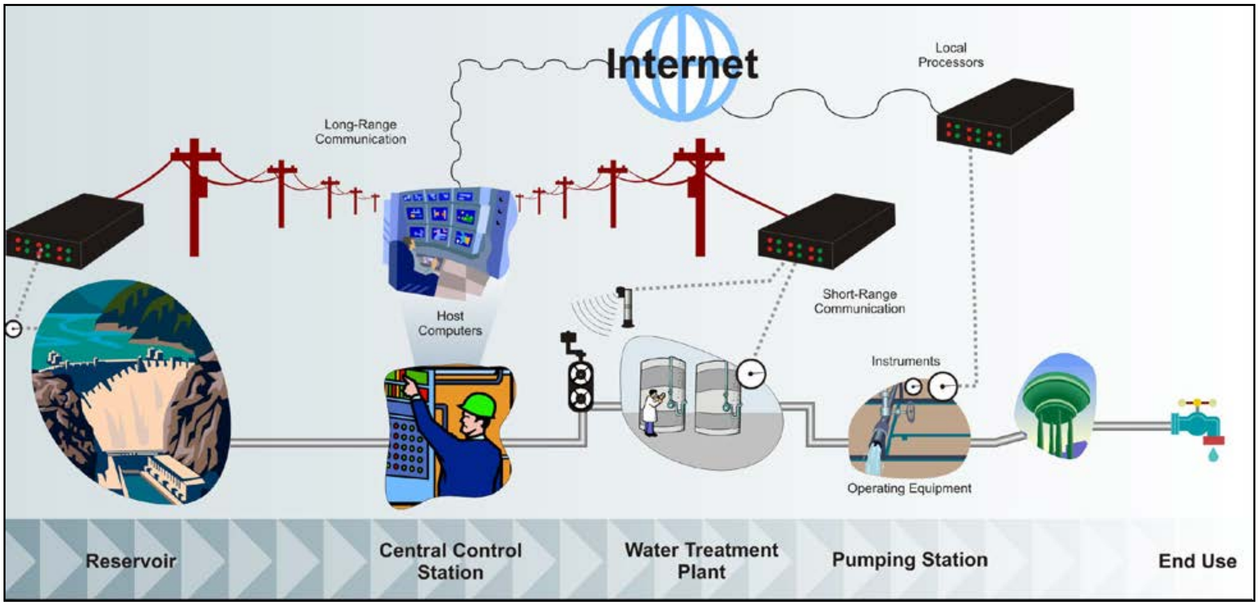
INFRASTRUCTURE SECTOR	SECTOR SPECIFIC AGENCY	KEY INDUSTRY GROUP
CHEMICAL	DHS	ACC
COMMERCIAL FACILITIES	DHS	BOMA
COMMUNICATIONS	DHS	
CRITICAL MANUFACTURING	DHS	
DAMS	DHS	TVA
DEFENSE INDUSTRIAL BASE	DOD	DIB
EMERGENCY SERVICES	DHS	APWA, NFPA
ENERGY	DOE	NERC, API
FINANCIAL SERVICES	DEPT OF TREASURY	
FOOD AND AGRICULTURE	DEPT OF AGRICULTURE & HHS	
GOVERNMENT FACILITIES	DHS & GSA	
HEALTHCARE AND PUBLIC HEALTH	HHS	
INFORMATION TECHNOLOGY	DHS	
NUCLEAR REACTORS, MATERIAL & WASTE	DHS	
TRANSPORTATION SYSTEMS	DHS & DOT	ASCE, AASHTO, API
WATER	EPA	AWWA

Examples of Successful Industry Collaboration

Leading work within two infrastructure sectors (water and electric power) provide risk management approaches useful for consideration by other infrastructure committees.

Water Systems.

The AWWA and DHS collaborated in defining a detailed strategy to mitigate cyber risks to our Nation's water systems. Roadmap to Secure Control Systems in the Water Sector developed by the Water Sector Coordinating Council Cyber Security Working Group presents a unified security strategy that can serve as a model for other industry sectors. This document provides the vision and supporting framework of goals and milestones for reducing the risk of ICS over the next ten years. The framework aligns industry and government programs and investments, improving ICS security quickly and efficiently. The roadmap integrates the insights and ideas across a broad cross-section of asset owners and operators, industrial control systems experts, and government leaders gathered from workshops in 2007. Addressing technical, business operations, and societal challenges, the roadmap gives water sector industry leaders the way forward to be able within ten years to manage a cyber event without loss of critical function.



Notional Components of Industrial Control Systems (ICS) for the Water Sector (Source: GAO 07-1036)

Electrical Power Grid.

NERC CIP Standards provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles in the operation of the grid, the criticality and vulnerability of the assets needed to reliably manage the grid, and their exposure risks. The operational demands of managing and maintaining the grid relies increasingly on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations. These connections result in increased risks to infrastructure systems, requiring cyber linkages be identified and managed through risk-based assessment.

Topics to be addressed within any industry sector include these:

- Emergency Operations Planning
- Responsibilities and Authorities
- Threats and Hazards Analysis
- Single Points of Failure
- Risk Assessment and Mitigation Measures
- Mission Assurance Monitoring
- Disturbance Monitoring
- Reliability Analytical Tools
- Communications and Coordination
- Disturbance/Event Reporting
- Alternative supplies/support
- Priorities of Response Effort
- Compliance Audits
- System Restoration Plans
- Reliability Assessments
- Loss of Control Center Function
- Continuity of Operations
- Facility Connection Requirements
- System Maintenance Management
- Mutual Aid Arrangements
- Open Source Threat Assessment
- Facility Condition Ratings
- System Operating Limits
- Transfer Capabilities
- Key/Critical Personnel

The Way Ahead

Developing a successful Framework requires the collaboration of stakeholders from affected industries as well as Government. It also requires integrated teams of practitioners from a wide variety of technical disciplines. The Industrial Control Systems that manage critical processes such as electric power generation, oil and gas refining, fuels pipelines, water and wastewater treatment, and chemical, air traffic control, food, and automotive production are the domain of mechanical, electrical, and civil engineers. However, since the cyber effects fall within the domain of IT disciplines, an integrated team of professionals is needed to understand the full complement of threats and hazards vulnerabilities in developing effective risk mitigation measures. Every identified critical infrastructure sector relies on ICS or related controls technology.

Use of ***Integrated Project Teams*** to identify best practices within industries will facilitate cross-fertilization of ideas and best business practices between industries; for example use of NERC’s approach as a common outline structure. The working committees are already established by industry sector groups (domestic and international) and associated federal agencies. These committees are responsible for CIP policy guidance developed and refined via collaboration and coordination with industry technical groups to define best practices and leverage private sector expertise in mitigating threats and hazards to critical infrastructure.

These committees address the eight components of the National Preparedness System.

- Target capabilities and preparedness priorities
- Equipment and training standards
- Training and exercises
- Comprehensive assessment system
- Remedial action management program
- Federal response capability inventory
- Reporting requirements
- Federal preparedness.

Evaluation of Risk and Risk-Reduction Options

Every action we take, every decision we make and every dollar we invest has an element of risk. No matter how much preparation we do or security we put in place there is still an unavoidable measure of risk. How ***we manage that risk*** is a function of how well we understand the threats, vulnerabilities, likelihood and consequences of the realization of that risk. Lately, the front page of every newspaper featured headlines about the grim and almost always unexpected realization of cyber risk. The positive outcome of this is that more owners and operators of Critical Infrastructure are becoming much more knowledgeable of the cyber "threat."   At least with the acknowledgement of a threat, people and organizations may be closer to moving towards an evaluation of that threat in their own context.

Even for Cybersecurity-savvy individuals and organizations, however, there is still a two-dimension view of the threat-risk dynamic. The common narrative of the responsible organization would be to try to understand the threat, try to understand their critical components, and figure out how to implement security to mitigate the threat. Test, rinse and repeat.   If the threat is big and the critical components are big, then add a lot more to the security architecture. This is appropriate, but there comes a point when the cost for implementing enough security to eliminate all risk is prohibitive. Further, the risk picture changes daily with evolving threats, technologies, missions, etc. There is no static security model that could comprehensibly protect an organization except for the briefest moments of time.   Integration lifecycles of new technologies that can protect against new threats takes a minimum of weeks if not months. So, no matter how well-protected an organization is at any one time, it will be unavoidably vulnerable to new, unexpected threats almost immediately. These are dangerous times and hazardous waters even for the most able of captains and ships.

What is needed is a mechanism that incorporates and rewards implementation of best security practices, leverages the collective threat and countermeasures knowledge of a broad community of practitioners, makes the community safer, and instantaneously and flexibly expands or contracts to fill the critical void where security countermeasures fail. Fortunately, there are some useful corollaries from related industries that can inform NIST as the new Framework is developed.

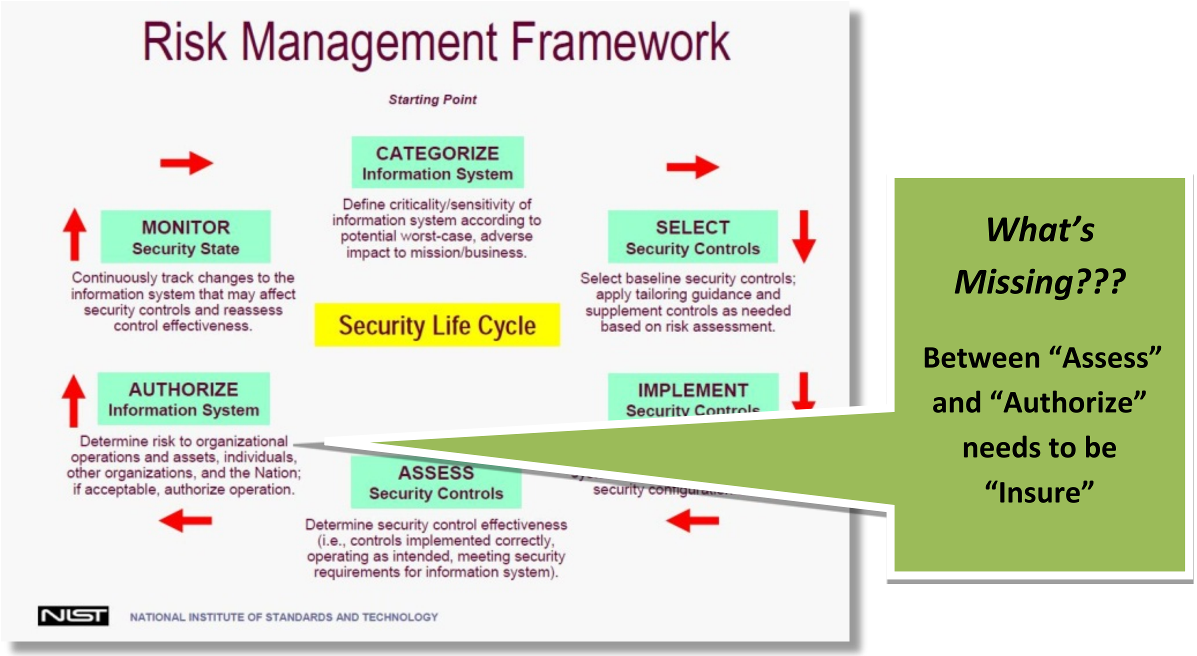
Cyber Risk Insurance

People have been dealing with formal concept of risk for almost all of recorded history. One can go back 4000 years to Babylonian and Chinese traders who collaborated to insure their ships against loss. Without this insurance mechanism, merchant shipping would have not been economically feasible. No amount of planning for weather or building the strongest ship could eliminate the risk entirely, and no one would want to invest in a voyage if there were not protections in place for loss. Those were dangerous times as well, as ships could be lost due piracy, theft, fire, warfare, weather, disease, famine, scurvy, or poor navigation. But there was an urgent need for commerce, so they had to find a way to operate despite the tremendous threats. These early traders knew enough to know they couldn't account for all the risk and knew they could not possibly protect against every threat, but through the concept of collective sharing of risk through insurance, they still found a way to function. Four millennia later, this institution is still in place and it still works.

This Framework affords an opportunity to consider new solutions to an urgent problem. In 2012, many organizations have awakened to the concept of cyber risk insurance. Sales of this risk reduction mechanism have risen 33% in the last year. This method or risk reduction is consistent with how other endeavors and industries have learned to deal with risk throughout history. This Framework should acknowledge this mechanism and incorporate its usage into an accepted tool for risk mitigation. This will move the concept of "cyber risk insurance" from a niche leveraged by only some forward-thinking executives to its proper role an essential pillar of a comprehensive risk management strategy for all companies including those in the Critical Infrastructure community. This is a necessary evolution of the art of risk management, and one that may ultimately turn the tide against the cyber threat that is undeniably winning today.

Today, information technology risk management in the U.S. bears the evolutionary DNA of IT security that began in the mainframe era for systems supporting the Federal Government and Department of Defense. Families of security controls were developed that addressed technical issues such as use of authentication, separation of duties, configuration of systems, etc. As the discipline evolved, non-technical controls, such as management, personnel security, security training and many others were developed to fill the gaps. These were documented in DoD and Federal Standards, such as NIST 800-53, but since the intended audiences of the publications were Federal and DoD agencies, "insurance" never even entered the vocabulary. Why would the guidelines prescribe a risk mitigation strategy that was unavailable for its implementers? An unintended consequence of the Federal focus for the guidelines is that they do not address the full gamut of solutions available to the commercial world which owns and operates over 80% of our Nation's Critical Infrastructure. Many commercial security managers and security officers look to these guidelines as the "gold standard" of security without realizing there are other options. "If it's good enough to protect classified defense systems, then it is certainly good enough for my human resources system!"

Current NIST Risk Management Framework



Risk Management Framework

Starting Point

CATEGORIZE Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

IMPLEMENT Security Controls

security configuration

ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

MONITOR Security State

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

What's Missing???

Between "Assess" and "Authorize" needs to be "Insure"

Introducing the additional step of "insure" in the Risk Management Framework is a logical and useful evolution of this iterative process. Even when the process of categorizing the system, selecting the security controls and implementing the controls is done to the highest standard, assessments almost always reveal that security vulnerabilities remain on the system. These vulnerabilities can be caused by the nature of the system; some systems must use protocols that are less secure than others and some necessary applications have vulnerabilities inherent in their software code. Sometimes, less secure settings, ports and protocols have to be used to meet operational requirements. The ultimate security posture of the system is always a compromise between security and functionality. Today, ideally, the manager is fully cognizant of the totality and severity of the vulnerabilities and the threat and makes the decision to accept the "residual risk."

"Residual Risk" is an accepted and much-vaunted concept in cyber security. There is an undeniable wisdom and philosophical harmony to the argument that we should do what we can do within reason and not feel too badly for what we can't improve. This concept of residual risk is nicely characterized by Reinhold Niebuhr's famous prayer, "God, grant me the serenity to accept the things I cannot change, the courage to change the things I can, and the wisdom to know the difference." Unfortunately, what may be true for individuals doesn't always translate to business. This philosophy can be little comfort for a Chief Information Security Officer (CISO) of a Critical Infrastructure organization when the "residual risk" quotient of their network lets a crippling attack destroy their computing infrastructure and data.

But what if that CISO could address his residual risk through a combination of insurance and shared risk-reducing threat information and security services?   What if CISOs could virtually eliminate residual risk? These security implementers should consider that there are more than technical and non-technical controls available to solve their problems. Instead of accepting an incomplete security solution, CISOs must gain awareness that risk mitigation is three-dimensional and that they have additional options.

Cyber risk insurance can bridge the gap between a company's intrinsic capability to absorb and mitigate a cyber event and their external financial obligation in the event of an incident.

As cyber risk insurance is more widely adopted, the insurance industry will begin to have an effect on defining and mandating safety and security standards for computing resources, just as they have with the auto industry, fire, and health. This is a positive influence to improve the overall security of all subscribers.

Risk Measurement and Analysis Methods

This Framework should address how risk is measured, and how "credit" is evaluated for Critical Infrastructure owners who implement non-traditional methods of risk reduction, such as cyber risk insurance. The effort to develop the Critical Infrastructure Framework should also investigate whether a new statistical method of calculating risk should be developed.

- The Framework workshops should include the compliance and certification and accreditation community to develop measurable standards and risk reduction metrics. How much "credit" is an organization given if it has insurance. Is there a limit to how heavily an organization can rely on insurance to buy-down their risk exposure? Is it 10%, 25%, 2%? There is much work to be done to develop a useful measure.
- The Framework workshops should also evaluate which risk analysis methods are most appropriate to Critical Infrastructure. The common methods in use today do not satisfactorily account for the "low probability, extremely high impact" events that characterize worst-case scenarios for Critical Infrastructure. Consider the difficulty in calculating the risk of another "Bhopal, India" type event that is triggered through a cyber event. Existing methods of risk analysis include the following:
    - Qualitative Risk Analysis

- Semi-quantitative Analysis
- Quantitative Analysis

Conclusions and Recommendations

Cybersalus and Alpha Terra Engineering, Inc. support NISTs effort to develop a useful framework to improve Cybersecurity for Critical Infrastructure. The threats are numerous and the risk to our Nation is grave. The outcome of this effort will provide a strong precedent to other industries and organizations.

NIST should look beyond the common tools in use by the Federal government to mitigate risk and evaluate whether the commercial world's adoption of cyber risk insurance is a useful element of an overall risk mitigation strategy. Collective risk aggregation through a mechanism such as insurance can help raise the overall security of the industry, but provide resiliency to the companies that suffer a cyber event.

Part of this Framework development effort will include a revamping of the risk measurement and analysis methodologies in practice today to properly account for the black swan scenarios that have a much higher impact than standard statistical analysis encompasses.

NIST should also include physical security experts in the development of the Framework to ensure that the physical risks to the information technology infrastructure are properly addressed.

About Us: The CYBERSALUS / ATEI TEAM

The Team of **CyberSalus** and **Alpha Terra Engineering** offer unique capabilities in both the physical and cyber realms of critical infrastructure protection. Because cyber risk management is parallel and complementary to physical and human-focused risk management, a **TEAM** with capabilities in both dimensions is essential to understanding full spectrum issues and initiatives. We have the broad ability to focus on people, processes, and technology in understanding cyber risk management in concert with other aspects of risk management.

Our SMEs possess the comprehensive background to understand how sector-specific strategic plans frame practical goals of providing resilience, diversity, redundancy and recoverability. We have the ability to operate technically at both 'tactical and strategic' levels.

Cybersalus LLC

CYBERSALUS LLC is a Service-Disabled Veteran-Owned Small Business (SDVOSB) that specializes in CYBER - to include both offensive and defensive cyber operations, technology and program management. We provide for thought leadership, security architecture, system engineering, strategic planning, acquisition policy, information technology, and program control. The CYBERSALUS Executive staff has senior management experience in managing numerous CYBER multi-agency initiatives.

Capabilities

CYBERSALUS's corporate commitment is to provide extraordinary CYBER experts and technology to operate and defend in the Federal, Defense, Intelligence and Commercial cyber space. Our staff focuses a shared commitment with each customer and provides collaborative efforts to ensure successful products, innovative solutions and personnel to meet all your Cyber challenges. Our capabilities cover:

Information Assurance
Cyber Threat Assessments
Security Architecture Consulting
Security Awareness Training
Identity Management
Intrusion Detection
Digital Forensics
Government Regulatory Compliance (GRC)
Certification and Accreditation
Network Security Operations
Incident Response
Contingency (COOP) Planning
Security Policy Development
PKI and SmartCard Implementation

And we are committed to:

1. Integrity
2. Quality solutions
   The Best Return On Investment (ROI) for your security expenditure.

Located in the Greater Washington DC Metropolitan, CYBERSALUS is currently standing up capabilities in Cyber Security and Information Services to support a range of customers to include the DOD, Homeland Security and Intelligence Agencies. CYBERSALUS is entrepreneurial and growth-oriented, and the direct result of a joint initiative of SKC LLC (a skilled logistics systems and support company in the Federal

Intelligence business) and McLane Advanced Technologies (MAT) Inc. (a highly successful software company in both the Commercial and Federal space.) These two partners form a firm financial foundation to quickly move Cyber Initiatives forward. We are leading-edge cyber technologists, open to creativity, agile to respond, and driven by the customer's needs above all else. Our solutions are not "black box" but the result of an open and continuous dialogue with the customer.

Finally, we are uniquely postured with both operationally experienced cyber experts as well as exclusive partnership use of a world-class advanced technology and software laboratory to quickly design, model, test, and implement divisive and innovative capabilities. As a small business, we offer the significant advantages of agility to respond, very low wrap-rates for our services, and reach-back to a deep bench of industry experts and computing resources that allow us to be completely responsive to meet Federal and Commercial CYBER challenges.

Key Officers

We are led by military Veterans - over 100 plus years of collective leadership in Cyber Security and operations.

John Kiehm

1. **John Kiehm is the CEO, CYBERSALUS** (and President and CEO of SKC) and a former Defense Intelligence Agency (DIA) Chief of Staff. In addition to his staff responsibilities, he directed the monumental reform of the agency's Human Resource program. During his career at DIA, Mr. Kiehm was charged with centralizing the management of Defense Human Intelligence and moreover, developed this service into an internationally respected organization. He implemented his vision of automating critical functions of its operations and management of records making the organization's critical intelligence products real time.

   Mr. Kiehm's last assignment was served as the senior DIA representative to the Supreme Allied Commander, NATO Forces and Commander of the U.S. Forces, European Command. He also served as the Director for Engineering and Logistics Services, providing critical operations support to include engineering and logistics services to CONUS-based activities of DIA as well as diplomatic support for defense attaché offices worldwide. Mr. Kiehm served in the U.S. Air Force as a commissioned officer for twenty four years and upon retirement, joined DIA in a civilian capacity.

Since retirement from DIA as a Senior Executive Service member, he served on corporate boards and provided consulting services for private and public corporations. His hands-on human source intelligence operations experience, logistical expertise, as well as internal knowledge of military operations, make Mr. Kiehm and SKC a valuable partner for customers seeking secure solutions in key mission areas.

Tom Verbeck

2. **Thomas Verbeck is President, CYBERSALUS**. A service disabled veteran, Mr. Verbeck brings over 37 years of extraordinary leadership in the Cyber space arena…rising to Brigadier General ,United States Air Force, and industry Chief Technical Officer (CTO.) He led air, communications, information systems in all aspects of military CYBER space; Chief of Staff/Director of Staff of Central Command Air Forces and Air Combat Command; culminating his 34 year military career as the first Combatant Command J3-Cyber operations (defense and offense)), European Command with responsibilities affecting more than 92 countries-EUROPE- AFRICA; Middle East and Southeast Asia. In addition, he was the J6 and J9 responsible for all Command, Control, Communications and Warfighting systems Integration. A lauded (Federal Top 100) Chief Information Officer (CIO) and Chief Technology Officer (CTO) , he has deep roots in the acquisition and program management of new divisive information technology systems and was responsible for standing up the first deployable network operations and security center (NOSC) in southwest Asia . A CYBER Lauded speaker and teacher, he taught in Europe and Africa; leading COMBINED ENDEAVOR (with over 50 European and EURASIAN Countries in IT inter-operability) and lead the standup of AFRICAN ENDEAVOR…the first Cyber; network interoperability exercise with 20 African Countries. He was the successful Program Manager for the Air Force $1Billion NEXRAD program and as an industry CTO; he pioneered, led development, and fielded the secure BLUE BUTTON APP for VA Health Records - a first for Veterans Health care! Tom Verbeck has a Master of Science, Systems Management from the University of Southern California, and Bachelor of Science in Electrical Engineering from Virginia Tech; a TS/SCI clearance, and is a graduate of the Industrial College of the Armed Forces, National Defense University.

Dana Shafie

3. **Dana Shafie is the Executive Vice President, Cybersalus**. He has more than 20 years in cyber security and operations with lauded experience as a Cyber Security Architect and Subject Matter Expert (SME) in information assurance, network security, certification and accreditation, and security watch operations.

   He was the lead Cyber Security Architect for many high profile programs to include the billion dollar Navy CANES contract, FAA Cyber Security Management Center, Defense Video Services Global IP-based Video Telecommunications Services, Navy Emergency Management System, Battlefield Area Communications Node, JSS Communications Node, FBI PKI, DOJ PKI.

   A former Navy Commander (O5), he had responsibility as a Cryptologic (Information Warfare) Officer; exchange officer to US Army INSCOM, airborne reconnaissance and Signals Intelligence expert and led crisis action cells at the National Security Operations Center, National Security Agency. He is a graduate of the Villanova and the Defense Intelligence Agency Joint Military Intelligence College for the Postgraduate Strategic Intelligence Program.

CYBERSALUS is ready today to tackle your smallest and biggest CYBER issues and provide quality solutions to meet the demands of our Federal and Commercial Market Place.

Alpha Terra Engineering, Inc. (ATEI)

ATEI has primary responsibility for the physical component of critical infrastructure protection with its experience derived from on-site DCIP program surveys under the Air Force's Critical Asset Risk Assessment (CARA) program and the Marine Corps' Mission Assurance Assessment (MAA) programs. Our staff has the requisite military background, technical engineering and expertise, and security clearances to immediately support CIP objectives within both public and private sectors. Our staff of senior engineers and security specialists have experience from full military and civil service careers in these specialty areas. Based on recent involvement in related Critical Asset Risk Assessment (CARA) work for the Air Force world-wide, the ATEI team is intimately familiar with policy and issues related to the Air Force's CIP program.

ATEI is a Service Disabled Veteran Owned Small Business established in 2005 by a former Air Force engineer officer. ATEI has recently supported the Air Force with engineering facilities assessments around the globe. ATEI completed assessments at more than 20,000 facilities at 84 military installations. ATEI's proposed staff for CIP work includes a strong cadre of senior professionals with years of Air Force Civil Engineer, Force Protection and Anti-Terrorism experience. ATEI services related to MA/VA include engineering design and analysis, utilities infrastructure, occupational health and safety, security engineering, force protection, anti-terrorism and law enforcement.

ATEI's experience with critical infrastructure protection derives from DoD Mission Assurance imperatives requiring a comprehensive and integrated framework to assess and manage risks to mission essential functions (MEFs). CIP objectives focus on protecting the resiliency of DoD missions to reduce the risks from the full spectrum of threats and hazards. Latest strategies for ensuring MA leverages existing vulnerability assessment methodologies incorporating anti-terrorism, physical security, defense critical infrastructure and information assurance into a new construct that measures the effectiveness of MA in terms of DoD's ability to continue performing its MEFs.

Many of MA issues are highly technical and require seasoned judgment by subject matter experts (SME) on military capability and the wide range of enemy, manmade and natural threats and hazards. Anticipating, detecting and identifying potential MEF stoppers require unconventional thinking of the full panoply of the all-threat and all-hazards environment. ATEI's DoD experience provides the capability and capacity to meet NIST's complex CIP requirements. We have direct working knowledge of Air Force, Army and USMC MA/VA organizations and recent MA/VA work experience with these three services at 15 major DoD installations. ATEI's staff brings full knowledge of CIP mission areas, plus hands-on expertise in many facets of those requirements.

ATEI offers an integrated, multi-disciplinary team of engineers and security specialists ready to provide advisory or assistance services or conduct the assessments. We are ready to meet and exceed customer expectations and successfully deliver qualified support services and professional products. Based on previous experience, our team has the specialized program understanding and 'hands-on' experience to conduct or support the CIP without the need for program 'spin-up'.

ATEI is postured to deliver immediate and comprehensive long-term support to the NIST. Our team provides a stable of seasoned practitioners with the requisite experience and credentials for successful CIP support.

ATEI offers NIST seasoned practitioners with unique understanding and capabilities able to support the Nation's CIP mission. We are experienced with the program and possess a broad understanding of the program's intent and mission mandate. Our team has worked hard to build a strong rapport with all services and service agents, and our team has earned the trust and confidence of both organizations. We are familiar with all aspects of increasingly complex demands in protecting our critical infrastructure from both natural and 'man-made' hazards and threats.

ATEI provides superior value:

☑ ATEI fully understands the CIP mission and organization

☑ Our team has the experience, capability, and capacity for successful CIP performance

☑ We provide full-spectrum CIP mission coverage (current exception IA)

ATEI is an experienced, proven Air Force contractor

☑ Three years and five task orders, including two sole source awards, under AFCEE's A&E program

☑ Back-filled deployed personnel eliminating loss of mission functions

☑ Experience that spans the entire range of CIP support

☑ Working familiarity with Air Force processes and priorities

☑ Every deliverable receives thorough, independent management reviews

Our Past Performance Demonstrates Excellence - ATEI is completing its sixth year of successful advisory and assistance consulting services for the Air Force.

☑ Successfully communicating highly technical information in a meaningful way to all stakeholders

☑ Highly experienced and qualified professionals who understand CIP requirements

☑ Epitomize the AF ethos of *Integrity First….Service Before Self….Excellence in All We Do*

Jorge Garza

- **Antiterrorism –** Jorge Garza has 27 years career experience in security, law enforcement, combat operations, anti-terrorism and force protection. He managed or maintained oversight of programs such as Air Force Anti-Terrorism Vulnerability Assessment Teams; Air Force Small Arms Program; Fraud Investigation Electronic Surveillance Teams; Procedures, Publications and Guidance for Air Force Security Forces Training; Security Forces Standardization and Evaluation and Air Force Policy for Anti-Terrorism and Force Protection.
- **Physical Security** – Jorge Garza managed security for Cheyenne Mountain and Eskan Village in Saudi Arabia. His responsibilities included perimeter security, entry/exit procedures and directing the response of security forces. Mr. Garza has experience with security of priority resources including nuclear assets, as well as aircraft alert areas and weapons storage areas.
- **Law Enforcement** – Jorge Garza was the Operations Officer at Offutt AFB and Commander at Cheyenne Mountain. Responsibilities included management and oversight of Visitor Control Centers, installation traffic flow, and day-to-day installation policing operations.
- **Defense Critical Infrastructure Program (DCIP) –** Fred Waterman is a registered professional Civil Engineer with over 30 years experience in military engineering, facility support and MILCON program management. He is a retired Army Reserve officer in the Corps of Engineers with 27 years experience including two overseas deployments. Over the last three years Mr. Waterman has completed CARAs at JB Andrews, Andersen, Eglin, Robins, Schriever, Vandenberg, Kirtland, and Tinker and comparable MAATs at MCB Quantico, MCAGCC 29 Palms, MCB Pendleton, MCAS Iwakuni, Camp Butler, MCAS Futenma, and MCLB Barstow. He completed CARA visits collecting data on utility and other critical nodes of infrastructure, assessing the threats to the infrastructure supporting key mission of the installation, and determining the risks resulting from those threats. The product of each CARA visit was a report describing those risks. Having a career in military engineering permitted him ability to quickly access types of information vital for effective assessments.
- **Installation Emergency Management –** ATEI is affiliated with Aktarius Technical Services (ATS), a Veteran Owned Small Business with principals having over two decades combined experience on staff at AFCESA and at the Air Staff Pentagon HAF/A7C in contingency support including functions such as readiness, explosive ordnance disposal, expeditionary engineering, fire and emergency services, and energy. ATS' extensive experience in hazardous materials operations, counter-explosive hazards, and force protection is unparalleled for a small business.
- **CBRNE –** DoD Instruction 2000.18 implements policy, assigns responsibilities, and prescribes procedures to establish and implement a program for worldwide DoD installation emergency response to manage the consequences of a CBRNE event.

Dr. James Lohaus

Dr. James Lohaus is a retired Air Force Bioenvironmental Engineer with a PhD in Civil Engineering and MS in Health Physics. Dr. Lohaus directed multi-agency, bio-aerosol research effort investigating exposure risks to airborne respiratory pathogens in US, and Iraqi and Afghani theaters. Dr. Lohaus designed, executed and reviewed for quality the radiological decontamination and decommissioning for the largest Air Force hospital. He has been a Medical Radiation Safety Officer (RSO); NRC Trustworthiness and Reliability Official; Visiting Professor, Air Force Institute of Technology (AFIT). Dr. Lohaus directed all research activities and ensured quality within the Department of Occupational/ Environmental Health, USAF School of Aerospace Medicine. He conducted and reviewed for quality health risk assessments, nuclear/biological/chemical (NBC) defense investigations and exposure surveillance for deployed personnel at garrison and deployed locations.

Fred Waterman, PE, CCM

Fred Waterman, PE, is Vice President and Principal Engineer of ATEI. Fred has over 30 years professional engineering experience in the federal sector with both the Army and Air Force. As the military construction program manager for US Air Force Europe, Fred successfully managed DoD's largest construction project. As a consequence of that success, he was contracted by Europe District of the Corps of Engineers to manage construction risk management planning for the replacement Landstuhl Regional Medical Center at Ramstein AB, Germany. While with Booz Allen Hamilton, Fred had conducted detailed Defense Critical Infrastructure Assessments of 15 Air Force and Marine Corps installations, specializing in risk mitigation of infrastructure supporting Tier I and II Task Critical Assets. Fred is a Registered Professional Engineer, Certified Construction Manager (CMAA) and Project Management Professional (PMP). He is a graduate of the National Defense University's National Security Management Course, Air War College and Defense Leadership Management Program. Fred's military awards include the Legion of Merit and Bronze Star.