Quantitative Metrics to Assess and Manage National Cyber Security Risk Using Risk Meter Software

M. Sahinoglu, S. Morton, C. Kelsoe, M. Eryilmaz

Auburn University at Montgomery (AUM), Maxwell AFB and ATILIM University
msahinog@aum.edu, smorton1@aum.edu, christopher.kelsoe@us.af.mil;
meltem_eryilmaz@atilim.edu.tr

Abstract: One of the severest threats facing the United States or all free nations today is the National Cyber Security in the new Cyber Space era. The astronomically high malicious attacks, reminiscent of 1950s cold war has triggered a cyber-cold war among the world's once peaceful nations. Given the increasing number of attempted and actual cyber security breaches, originating from both criminal organizations and state-sponsored ones, and the very real as well as potential consequences ranging from financial loss to the catastrophic, make this threat undeniably and urgently addressed. In this work, a software tool to facilitate assessment and management of this unprecedented global threat is proposed. The National Cyber Security Risk Meter provides this critical tool for policy makers. Using game theory and statistically-driven methodologies, it provides objective, quantitative risk assessment, and unlike any other tool available today, guidance for allocating resources for risk mitigation. As such, decision and policy makers in government and industry will be greatly aided in their efforts to achieve greater cyber security by the use of this rational and objective tool for assessing and mitigating risk.

I. INTRODUCTION

Current national threats can range from mischievous lone hackers up the scale to organized cyber-criminal gangs to state sponsored cyber-espionage and cyber-terrorism. The economic damage inflicted to individuals, corporations, and the national infrastructure is put globally at $300 billion to $1 trillion globally [1]. But beyond mere economic impact, the potential damage could be globally catastrophic as in the nightmare scenario of multiple nuclear facilities' SCADA (Supervisory Control and Data Acquisition) systems being taken over simultaneously and causing uncontrolled meltdowns that could blanket entire continents in radioactivity. Such an event would make Chernobyl pale in comparison. To minimize and avoid such threats and potential damage, a rational, scientific approach that identifies, assesses, and manages national cyber security threats is required.

The identification and management of risk is the essence of cyber security. The National Cyber Security Risk Meter tool proposed here provides a unique and objective methodology that is critically needed. This pioneering work represents a paradigm shift in risk assessment. The National Cyber security Risk Meter provides a quantitative risk assessment, unlike the subjective high-medium-low or red-yellow-green scales commonly seen in other assessment methodologies. While there are other approaches to identifying and managing risk such as the National Institute of Standards and Technology's Common Vulnerability Scoring System (CVSS) [2], none provide a means of allocating risk mitigation expenditures. In contrast, the National Cyber Security Risk Meter provides objective and scientific guidance in allocating monetary resources for managing risk in accordance with budgetary constraints. Additionally, the National Cyber Security Risk Meter provides a means to shift from often subjective and crude risk evaluation mechanisms to a verifiable, quantitative approach to risk management, resulting in an optimized expenditure of security remediation dollars.

In this research, a model of national cyber security risk that quantifies the respondent's experience with eight crucial aspects of national cyber security is adopted. Those responses are subsequently used to calculate the national cyber security risk index through a designed algorithm by the principal author. To accomplish this task, numerical and/or cognitive data was collected from 34 respondents to supply the input parameters to calculate the quantitative security risk index for national cyber security. This paper will not only present a quantitative model but also provide a remedial cost-optimized game-theoretic analysis about how to bring an undesirable risk down to a user-determined "tolerable level". Lastly, it is an adaptable framework that can be customized and configured by the analyst with no custom coding (XML inputs).

II. METHODOLOGY

This applied research implements a methodology on how to reduce national cyber security risk. A software-centered holistic approach is proposed to aid computer security personnel, facility managers, decision and policy makers in identifying, assessing, and managing cyber security risk. Eight vulnerabilities are assessed: Energy Facilities, Transport Hubs, Internet, Government Net, Military Installations, Financial Net, Health Institutions, and Water Supply/Food Chain. Within each vulnerability category, questions pertain to specific threats and countermeasures. For example, within the Energy Facilities vulnerability, respondents are asked questions regarding Power Lines, Control Facilities, Hydroelectric, Fossil Fuels, and Nuclear Power threats and countermeasures. Within the Internet vulnerability, respondents are asked questions regarding Physical Network, Domain Name Servers, Other servers, Hacking, Denial of Service, Other Cyber Attacks, and Viruses threats and countermeasures. See Figure 1 below for the National Cyber Security Risk diagram detailing vulnerabilities and threats. The respondents' answers are then used to generate a quantitative national cyber security risk index.

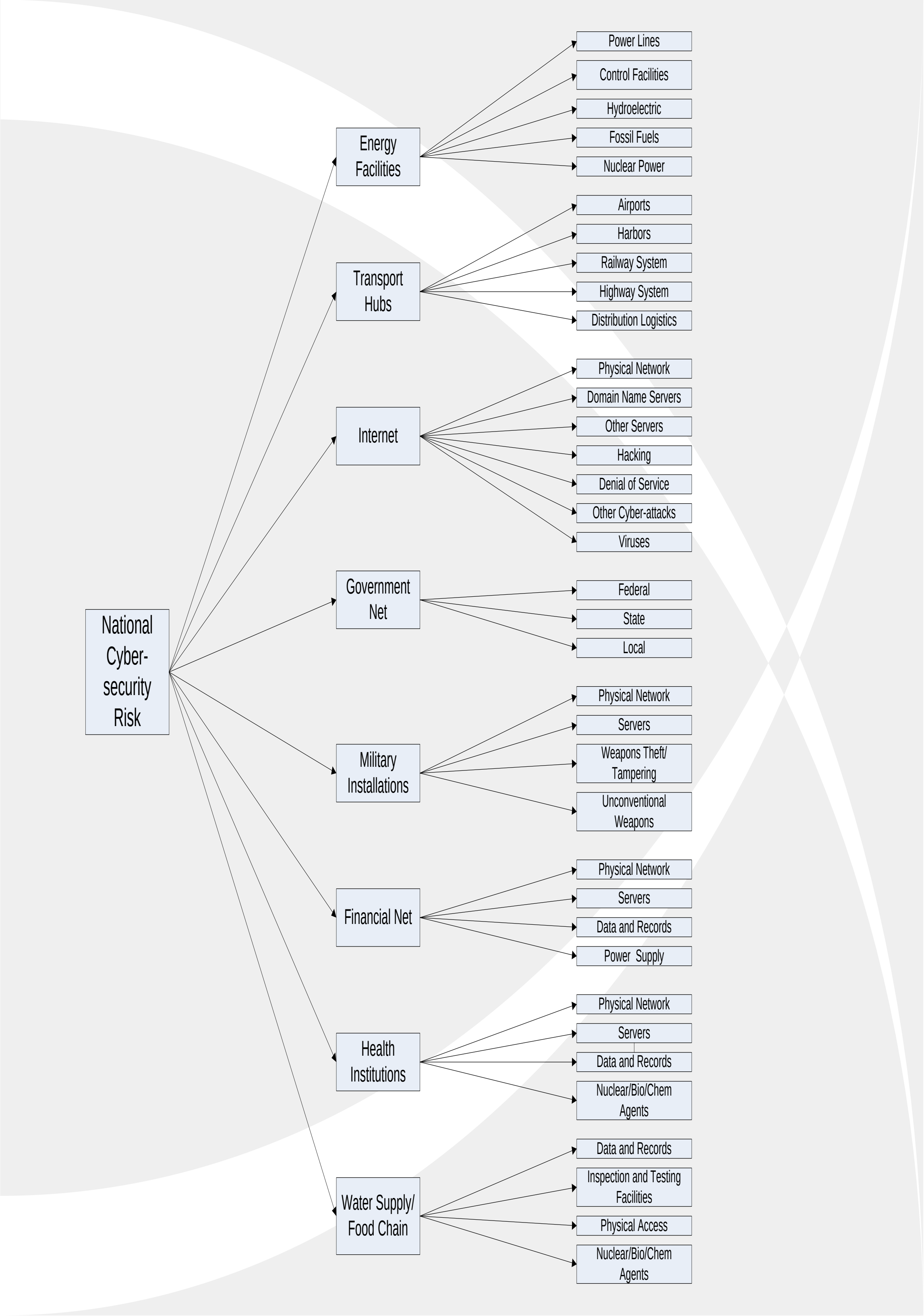


Figure 1: National Cyber Security Risk Tree Diagram.

Figure 1: National Cyber Security Risk Tree Diagram.

The primary author's innovation, i.e. National Cyber Security Risk Meter (an automated software tool), will provide computer security personnel, facility managers, decision and policy makers a measurable assessment of their current cyber security risk as well as detailing associated cost and risk mitigation suggestions for identified vulnerabilities and threats. The National Cyber Security Risk Meter will be demonstrated to provide such assessment and guidance for the allocation of resources for mitigating that risk. The cyber security metric out of 100% will be assessed and a remedial cost-optimized game-theoretic analysis provided to bring an undesirable risk down to a user-determined "tolerable level".

The approach the authors propose here is a game theoretical-based approach that emphasizes the quantitative analysis of vulnerabilities, threats and countermeasures shown in Figure 1 above. The theoretical framework behind the National Cyber Security Risk diagram shown there is a tree diagram with vulnerability branches, threat twigs, and countermeasure branches that calculates total residual risk as elaborated by Sahinoglu [3, 4]. This framework allows for the quantitative analysis of vulnerabilities and threats and the cost-optimal allocation of resources to countermeasures to mitigate or lower the risk from those vulnerabilities and threats. The framework is used by the National Cyber Security Risk Meter software tool described in the next section to output total residual risk. Note that RR (residual risk) = Risk of Vulnerability * Risk of Threat * Risk of Lack of Countermeasure. TRR (Total Residual Risk) is sum of RRs as in Figure 2 below.

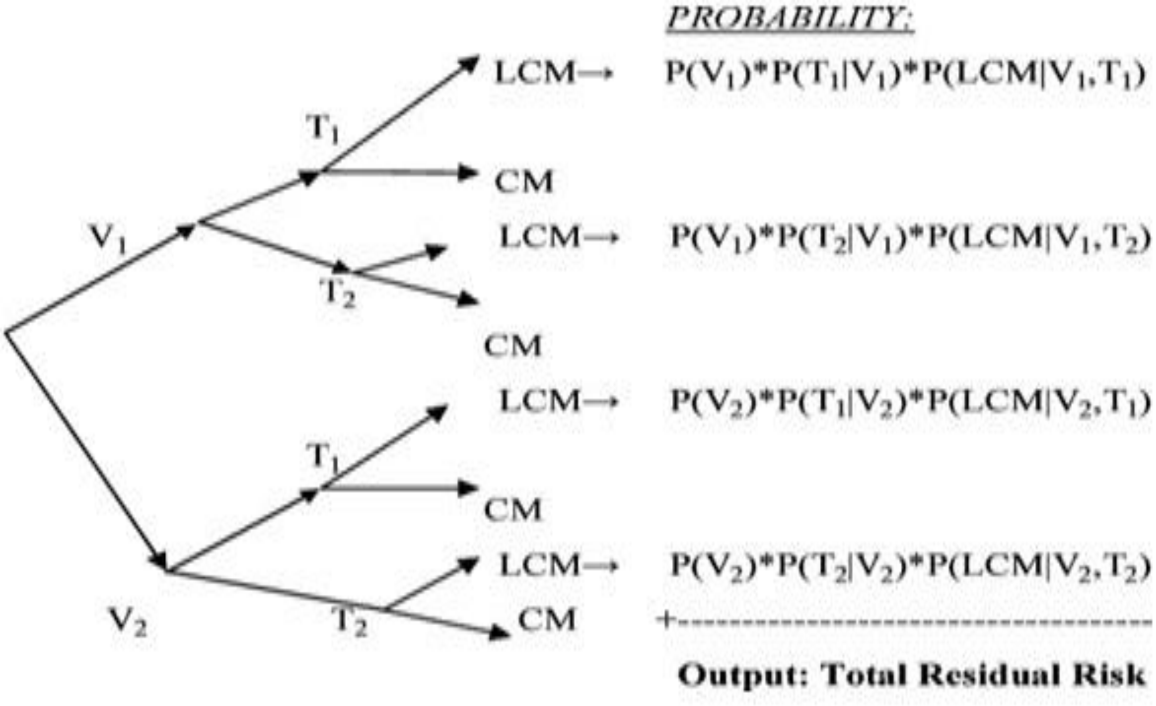

PROBABILITY:
LCM→ $P(V_1)*P(T_1|V_1)*P(LCM|V_1,T_1)$
T_1
CM
V_1
LCM→ $P(V_1)*P(T_2|V_1)*P(LCM|V_1,T_2)$
T_2
CM
LCM→ $P(V_2)*P(T_1|V_2)*P(LCM|V_2,T_1)$
T_1
CM
LCM→ $P(V_2)*P(T_2|V_2)*P(LCM|V_2,T_2)$
V_2
T_2
CM
+-----------------------------------
Output: Total Residual Risk

Figure 2. General tree diagram (V-branches, T-twigs, LCM-limbs) used for National Cyber Security Risk Meter.

While the National Cyber Security Risk Meter can be utilized on virtually any aspect of infrastructure or type of facility, this particular implementation focuses on eight key areas critical in ensuring national cyber security.

- Energy Facilities: Fundamental to daily life as well as security, the need to secure these facilities is critical given the potential damage should something go awry. This key area focuses on Power Lines, Control Facilities, Hydroelectric, Fossil Fuels, and Nuclear Power. Each of these areas must be addressed to ensure continued and undisrupted national operations.
- Transport Hubs: This area focuses on the facilities integral to transporting people as well as goods and services nationally, i.e.: Airports, Harbors, Railway Systems, Highway Systems, and Distribution logistics.
- Internet: Critical to not only modern commerce but control and communications as well, this key infrastructural component must be secured to prevent intellectual property, financial and physical loss. This key area focuses on Physical Network, Domain Name Servers, Other Servers, Hacking, Denial of Service, Other Cyber Attacks, and Viruses/Malware.
- Government Net: Assuring the integrity, availability, authenticity of governmental and associated contractors' networks is critical to national security. This key area focuses on Federal, State, and local facilities.
- Military Installations: Critical because of the potential damage from misuse of weaponry and facilities, the need to keep unauthorized/unwanted individuals from gaining access to systems via electronic means as well as protecting the facilities that house these platforms must be ensured. This key area focuses on Physical Network, Servers, Weapons Theft/Tampering, and Unconventional Weapons.
- Financial Net: Critical to ensuring the daily life of citizens and the economy as a whole, this key infrastructural component must be secured to prevent financial loss and maintain a healthy economy. This key area focuses on Physical Network, Servers, Data and Records, and Power Supply.
- Health Institutions: Essential for preserving the population's health and well being as well as patient confidentiality, this key area focuses on Physical Network, Servers, Data and Records, and Nuclear/Bio/Chem Agents.
- Water Supply/Food Chain: Also essential for a nation's health and well being, contamination of water and food supplies must be prevented. This key area focuses on Data and Records, Inspection and Testing Facilities, Physical Access, and Nuclear/Bio/Chem Agents

While these eight areas are not exhaustive, they are relatively comprehensive of and critical to national cyber security. This research focuses on the areas vital to national cyber security and provides computer security personnel, facility managers, decision and policy makers with an analytical framework they can use to more efficiently secure their resources and facilities.

III. ASSESSMENT QUESTIONS

Questions are designed to elicit the user's response regarding the perceived risk to national cyber security from particular threats, and the countermeasures the users may employ to counteract those threats. For example, in the Energy Facilities vulnerability, questions regarding Control Facilities include both threat and countermeasure questions. Threat questions would include:

- Does your utility use an Ethernet-based Substation Automation System (SAS)?
- Does your utility fail to adhere to industry standards for reducing the risks from compromise of cyber assets?
- Does your utility use a Supervisory Control and Data Acquisition System (SCADA)?
- Can relay settings be accessed through the SAS user interface?
- Can the SAS server be remotely accessed over the internet?

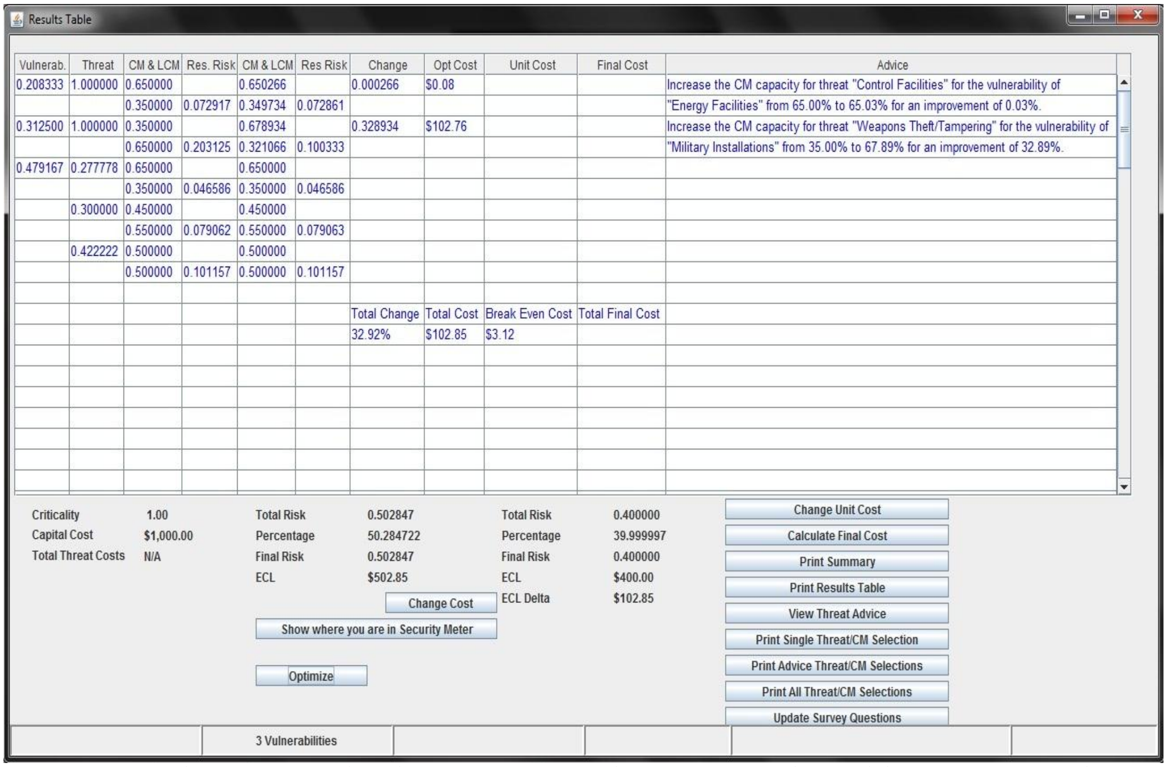
While countermeasure questions would include:

- Is your utility's SAS firewall and password protected?
- Has your utility implemented NERC CIP standards and policies to reduce the risks to critical cyber assets?
- Has your utility implemented higher security levels for its SCADA?
- Is your utility SAS user interface for relay settings password protected using special character, uppercase/lowercase combinations, etc?
- Is your utility's SAS server password protected using special characters, uppercase/lowercase combinations, etc.?

Please see Appendix B for a list of threat and countermeasure questions.

IV. RISK CALCULATION AND MITIGATION

Essentially, the users are responding yes or no to these questions. These responses are used to calculate residual risk. Using a game-theoretical mathematical approach, the calculated risk index is used to generate an optimization or lowering of risk to desired levels [3, 4]. Further, mitigation advice will be generated to aid computer security personnel, facility managers, decision and policy makers, and other interested parties in mitigation and resource allocation decisions. That is, in what areas can the risk be reduced to optimized or desired levels such as from 50% to 40% in the screenshot representing the median response from the study participants. See Figure 3 below for a screenshot of the Median National Cyber Security Risk Meter Results Table displaying threat, countermeasure, and residual risk indices; optimization options; as well as risk mitigation advice. For this study, a random sample of 34 respondents was taken and their residual risk results are tabulated and presented in Appendix A at the end of this paper. Respondents' familiarity with national cyber security risk included corporate, governmental, and military experience.



Vulnerab.	Threat	CM & LCM	Res. Risk	CM & LCM	Res Risk	Change	Opt Cost	Unit Cost	Final Cost	Advice
0.208333	1.000000	0.650000		0.650266		0.000266	$0.08			Increase the CM capacity for threat "Control Facilities" for the vulnerability of
		0.350000	0.072917	0.349734	0.072861					"Energy Facilities" from 65.00% to 65.03% for an improvement of 0.03%.
0.312500	1.000000	0.350000		0.678934		0.328934	$102.76			Increase the CM capacity for threat "Weapons Theft/Tampering" for the vulnerability of
		0.650000	0.203125	0.321066	0.100333					"Military Installations" from 35.00% to 67.89% for an improvement of 32.89%.
0.479167	0.277778	0.650000		0.650000						
		0.350000	0.046586	0.350000	0.046586					
	0.300000	0.450000		0.450000						
		0.550000	0.079062	0.550000	0.079063					
	0.422222	0.500000		0.500000						
		0.500000	0.101157	0.500000	0.101157					
						Total Change	Total Cost	Break Even Cost	Total Final Cost	
						32.92%	$102.85	$3.12		

Criticality	1.00	Total Risk	0.502847	Total Risk	0.400000
Capital Cost	$1,000.00	Percentage	50.284722	Percentage	39.999997
Total Threat Costs	N/A	Final Risk	0.502847	Final Risk	0.400000
		ECL	$502.85	ECL	$400.00
				ECL Delta	$102.85

3 Vulnerabilities

Change Cost
Show where you are in Security Meter
Optimize
Change Unit Cost
Calculate Final Cost
Print Summary
Print Results Table
View Threat Advice
Print Single Threat/CM Selection
Print Advice Threat/CM Selections
Print All Threat/CM Selections
Update Survey Questions

Figure 3. Median National Cyber Security Risk Meter Results Table (See Appendix A).

V. CONCLUSION AND DISCUSSIONS

Cyber space has quickly become the domain of primary concern for current national security concerns for all industrialized nations. Following the events of 9/11, emerging terrorist threats against food and water supplies, electricity and national networking capability sparked a review of the US critical infrastructure. The National Cyber Security Risk Meter breaks new ground in that it provides a quantitative assessment of risk to the user as well as recommendations for mitigating that risk. As such, it will be a highly useful tool for computer security personnel, facility managers, decision and policy makers, as well as other interested parties seeking to minimize and mitigate national cyber security risk in an objective, quantitatively-based manner. Future work will involve the incorporation of new vulnerabilities and additional questions so as to better refine user responses and subsequent calculation of risk and mitigation recommendations. Minimization and mitigation of national cyber security risk will greatly benefit not only the organizations deploying the tool, but society at large through the minimization of security breaches leading to intellectual property, financial and physical loss. The National Cyber Security Risk Meter tool and its future refinement provide the means to do so. The results for the median and mean surveys indicate that control facilities and weapons storage/protection are vulnerabilities that require the most attention. Military installations have rules and regulations on the protection of weapons and critical infrastructure. Since most of these rules and regulations were not in place when certain facilities, to include armories, were constructed, it may not be possible to implement the rules. This could be due to environmental impacts, overall facility construction, or adjacent facilities. Sometimes implementing the new rules and regulations are extremely cost prohibitive. Military Installations will typically conduct a vulnerability assessment and make a decision to either implement compensatory measure, or just waive the requirement for a specific facility. Respondents to this survey were aware of waivers and compensatory measures, but still indicated a vulnerability to those areas.

Respondents seemed to believe the survey served a valuable purpose. Most were a bit apprehensive about answering questions about vulnerabilities to a military installation. Military Installations undergo multiple vulnerability assessments and evaluations. All military installations have their own in house expertise on such matters; moreover there is extensive guidance from the Joint Staff and Headquarters Air Force on how vulnerabilities will be addressed. Future studies using the National Cyber Security survey as the focus Security Policy Seminar should focus their efforts on federal agencies outside the military, as well as state and local government agencies.

VI. REFERENCES

[1] Center for Strategic and International Studies (CSIS), “The Economic Impact of Cybercrime and Cyber Espionage”, Washington, DC July 2013.

[2] National Institute of Standards and Technology, National Vulnerability Database, “Common Vulnerability Scoring System” http://nvd.nist.gov/cvss.cfm (Accessed 4/25/2014)

[3] M. Sahinoglu, Trustworthy Computing, John Wiley, 2007.

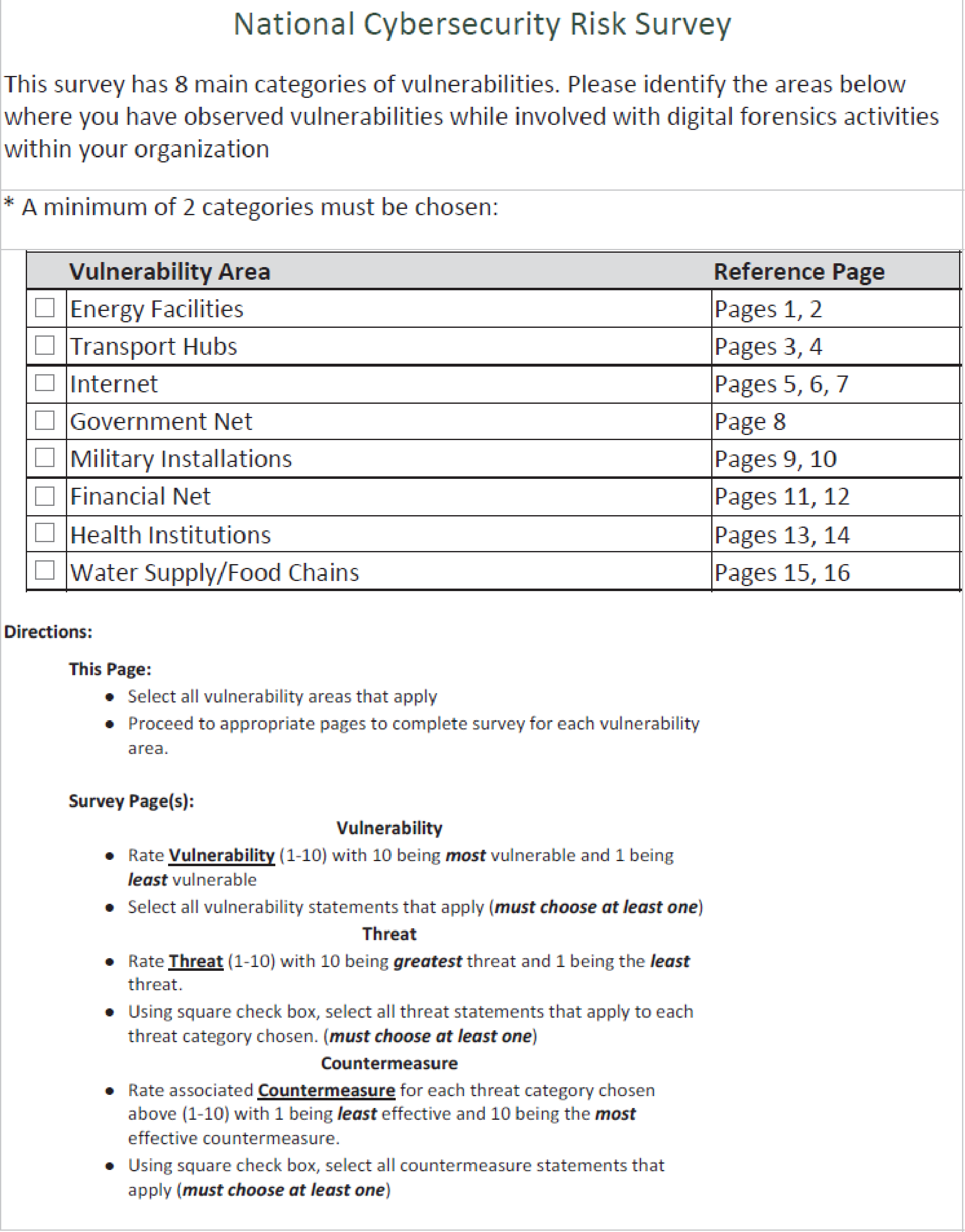
[4] M. Sahinoglu, “An Input-Output Measurable Design for the Security Meter Model to Quantify and Manage Software Security Risk”, IEEE Transactions on Instrumentation and Measurement, Vol. 57, No. 6, pp. 1251-1260, June 2008.

Appendix A: Respondent (Companies A, B, C) Residual Risk Results Table 1, Survey Results for the National Cyber-security Risk Meter study, ranked within and overall, where Median: 50.28% (B10) and Average: 48.86% (B6: 48.58% is the result that comes the closest) in the descending order..

SURVEY TAKER	RESIDUAL RISK %	RANKED OVERALL (OUT OF 34)	REMARKS
Company A1	51.98	8th	1st out of 13 within Company A
Company A2	44.41	29th	8th out of 13 within Company A
Company A3	48.23	21st	4th out of 13 within Company A
Company A4	50.34	17th	3rd out of 13 within Company A
Company A5	46.57	27th	7th out of 13within Company A *(Group Median for Company A)*
Company A6	42.67	31st	10th out of 13 within Company A
Company A7	47.14	24th	5th out of 13 within Company A
Company A8	42.94	30th	9th out of 13 within Company A
Company A9	39.01	34th	12th out of 13 within Company A
Company A10	42.25	32nd	13th out of 13 within Company A
Company A11	51.07	11th	2nd out of 13 within Company A
Company A12	40.21	33rd	11th out of 13 within Company A
Company A13	46.59	26th	6th out of 13 within Company A
Company B1	50.83	13th	6th out of 14 within Company B
Company B2	51.06	12th	5th out of 14 within Company B
Company B3	54.55	2nd	2nd out of 14 within Company B
Company B4	47.45	22nd	13th out of 14 within Company B
Company B5	52.69	7th	4th out of 14 within Company B
Company B6	48.58	19th *~OVERALL AVERAGE*	11th out of 14 within Company B
Company B7	54.17	4th	3rd out of 14 within Company B
Company B8	55.03	1st	1st out of 14 within Company B
Company B9	50.66	14th	7th out of 14 within Company B
Company B10	50.28	18th = *OVERALL MEDIAN*	10th out of 14 within Company B
Company B11	29.77	20th	12th out of 14 within Company B
Company B12	50.38	16th	9th out of 14 within Company B
Company B13	50.64	15th	8th out of 14 within Company B *(Group Median for Company B)*
Company B14	47.03	25th	14th out of 14 within Company B
Company C1	44.92	28th	7th out of 7 within Company C
Company C2	51.77	9th	4th out of 7 within Company C *(Group Median for Company C)*
Company C3	53.12	6th	3rd out of 7 within Company C

Company C4	54.43	3rd	1st out of 7 within Company C
Company C5	47.41	23rd	6th out of 7 within Company C
Company C6	51.38	10th	5th out of 7 within Company C
Company C7	53.28	5th	2nd out of 7 within Company C

Appendix B: Vulnerability, Threat and Countermeasure Questions



National Cybersecurity Risk Survey

This survey has 8 main categories of vulnerabilities. Please identify the areas below where you have observed vulnerabilities while involved with digital forensics activities within your organization

* A minimum of 2 categories must be chosen:

	Vulnerability Area	Reference Page
□	Energy Facilities	Pages 1, 2
□	Transport Hubs	Pages 3, 4
□	Internet	Pages 5, 6, 7
□	Government Net	Page 8
□	Military Installations	Pages 9, 10
□	Financial Net	Pages 11, 12
□	Health Institutions	Pages 13, 14
□	Water Supply/Food Chains	Pages 15, 16

Directions:

This Page:

- Select all vulnerability areas that apply
- Proceed to appropriate pages to complete survey for each vulnerability area.

Survey Page(s):

Vulnerability

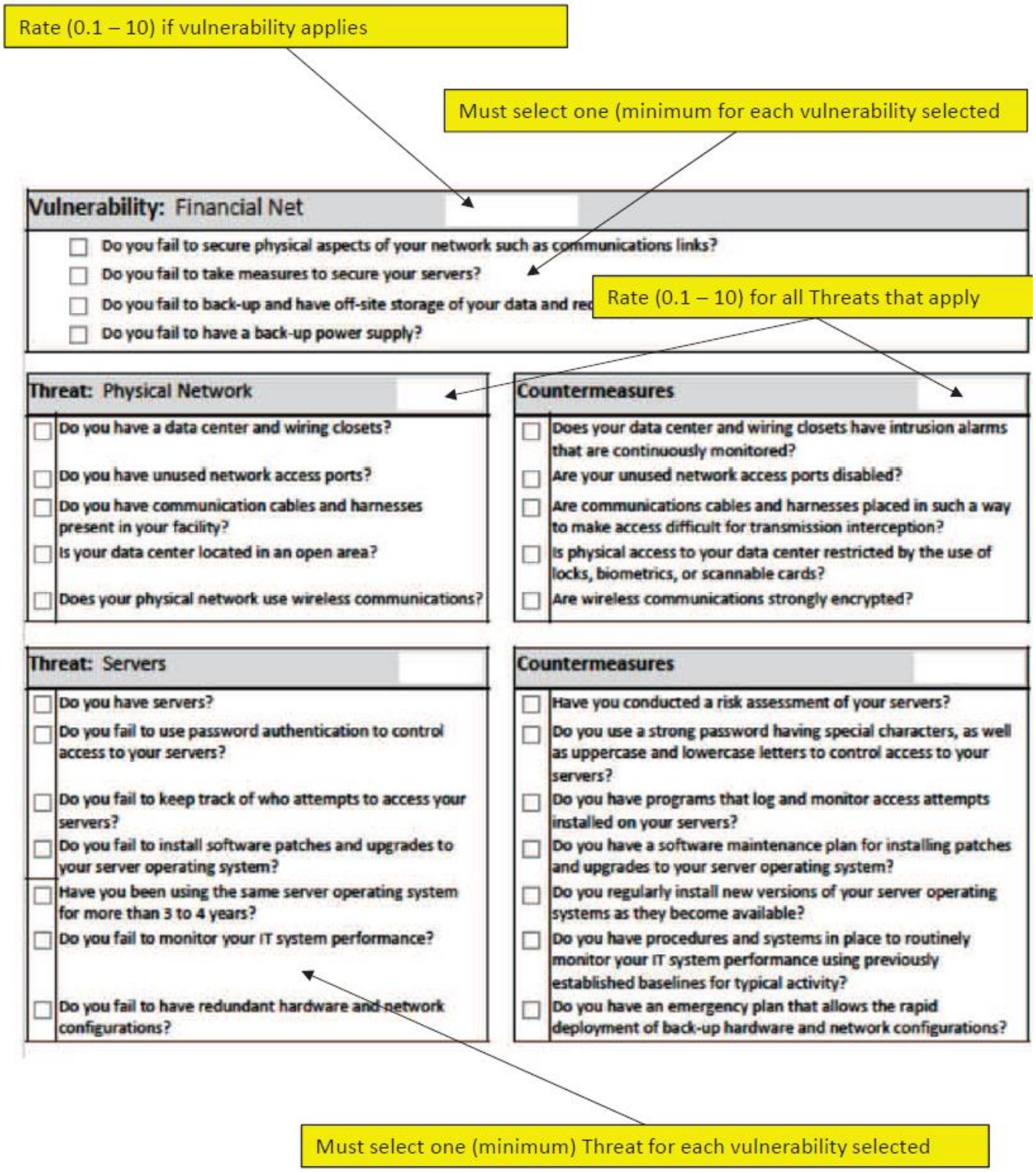
- Rate **Vulnerability** (1-10) with 10 being ***most*** vulnerable and 1 being ***least*** vulnerable
- Select all vulnerability statements that apply (***must choose at least one***)

Threat

- Rate **Threat** (1-10) with 10 being ***greatest*** threat and 1 being the ***least*** threat.
- Using square check box, select all threat statements that apply to each threat category chosen. (***must choose at least one***)

Countermeasure

- Rate associated **Countermeasure** for each threat category chosen above (1-10) with 1 being ***least*** effective and 10 being the ***most*** effective countermeasure.
- Using square check box, select all countermeasure statements that apply (***must choose at least one***)



Rate (0.1 – 10) if vulnerability applies

Must select one (minimum for each vulnerability selected

Vulnerability: Financial Net

- □ Do you fail to secure physical aspects of your network such as communications links?
- □ Do you fail to take measures to secure your servers?
- □ Do you fail to back-up and have off-site storage of your data and rec
- □ Do you fail to have a back-up power supply?

Rate (0.1 – 10) for all Threats that apply

Threat: Physical Network	**Countermeasures**
□ Do you have a data center and wiring closets?	□ Does your data center and wiring closets have intrusion alarms that are continuously monitored?
□ Do you have unused network access ports?	□ Are your unused network access ports disabled?
□ Do you have communication cables and harnesses present in your facility?	□ Are communications cables and harnesses placed in such a way to make access difficult for transmission interception?
□ Is your data center located in an open area?	□ Is physical access to your data center restricted by the use of locks, biometrics, or scannable cards?
□ Does your physical network use wireless communications?	□ Are wireless communications strongly encrypted?

Threat: Servers	**Countermeasures**
□ Do you have servers?	□ Have you conducted a risk assessment of your servers?
□ Do you fail to use password authentication to control access to your servers?	□ Do you use a strong password having special characters, as well as uppercase and lowercase letters to control access to your servers?
□ Do you fail to keep track of who attempts to access your servers?	□ Do you have programs that log and monitor access attempts installed on your servers?
□ Do you fail to install software patches and upgrades to your server operating system?	□ Do you have a software maintenance plan for installing patches and upgrades to your server operating system?
□ Have you been using the same server operating system for more than 3 to 4 years?	□ Do you regularly install new versions of your server operating systems as they become available?
□ Do you fail to monitor your IT system performance?	□ Do you have procedures and systems in place to routinely monitor your IT system performance using previously established baselines for typical activity?
□ Do you fail to have redundant hardware and network configurations?	□ Do you have an emergency plan that allows the rapid deployment of back-up hardware and network configurations?

Must select one (minimum) Threat for each vulnerability selected

Vulnerability: Energy Facilities

□ Do you fail to take measures to protect edges (transmission lines)?

□ Do you fail to take measures to protect strategic points such as control facilities?

□ Do you fail to take measures to protect hydroelectric facilities?

□ Do you fail to take measures to protect fossil fuel facilities such as refineries, pumping stations, and pipelines?

□ Do you fail to take measures to protect nuclear power facilities?

Threat: Power Lines	**Countermeasures**
□ Do power lines fail to be regularly inspected and maintained?	□ Do you have a routine inspection and maintenance plan for power lines?
□ Do power line substation nodes have excessive loads?	□ Are efforts being made to reduce excessive power line substation node loads?
□ Does the power grid system have a high level of connectiveness?	□ Are efforts being made to limit local disturbance propagation due to a high level of connectiveness?
□ Does the power grid lack redundancy?	□ Are efforts being made to increase the level of power grid redundancy?
□ Can high load substations readily fall in sequence?	□ Are safeguards in place to prevent cascading failures by high-load substations?

Threat: Control Facilities	**Countermeasures**
□ Does your utility use an Ethernet-based Substation Automation System (SAS)?	□ Is your utility's SAS firewall and password protected?
□ Does your utility fail to adhere to industry standards for reducing the risks from compromise of cyber assets?	□ Has your utility implemented NERC CIP standards and policies to reduce the risks to critical cyber assets?
□ Does your utility use a Supervisory Control and Data Acquisition System (SCADA)?	□ Has your utility implemented higher security levels for its SCADA?
□ Can relay settings be accessed through the SAS user interface?	□ Is your utility SAS user interface for relay settings password protected using special character, uppercase/lowercase combinations, etc?
□ Can the SAS server be remotely accessed over the internet?	□ Is your utility's SAS server password protected using special characters, uppercase/lowercase combinations, etc.?

Threat: Hydroelectric	**Countermeasures**
□ Has your hydroelectric facility's operator failed to assess the risk and potential for harm that could result from, unauthorized access and consequent disruption of their information systems?	□ Is your hydroelectric facility's operator in compliance with FISMA (Federal Information Security Management Act) and consequently developed a risk-based information security program as well as implementing information security controls?
□ Are control systems located in an open area?	□ Are control systems placed in secured, physical access-limited areas?
□ Does your hydroelectric facility have remote access systems?	□ Are control systems placed in secured, physical access-limited areas?
□ Does your hydroelectric facility fail to have an intrusion detection system?	□ Has your hydroelectric facility implemented and continuously monitors an intrusion detection system?
□ Does your hydroelectric facility fail to separate network segments?	□ Are separated network segments firewall and password protected to prevent access from a less secure segment?

Vulnerability: Energy Facilities (Continued)

Threat: Fossil Fuels	Countermeasures
□ Has your refinery operator failed to assess the risk and potential for harm, that could result from unauthorized access and consequent disruption of their information systems?	□ Is your fossil fuels facility's operator in compliance with FISMA (Federal Information Security Management Act) and consequently developed a risk-based information security program as well as implementing information security controls?
□ Does your gas turbine power generation facility use a Supervisory Control and Data Acquisition System (SCADA)?	□ Has your gas turbine power generation facility implemented higher security levels for its SCADA?
□ Are control systems located in an open area?	□ Are control systems placed in secured, physical access-limited areas?
□ Does your fossil fuels facility have remote access systems?	□ Are remote access systems firewall and password protected?
□ Does your pipeline network use an Ethernet-based Substation Automation System (SAS) for pumping?	□ Are your pipeline network's SAS firewall and password protected?

Threat: Nuclear Power	Countermeasures
□ Has your nuclear power facility's operator failed to assess the risk and potential for harm that could result from unauthorized access and consequent disruption of their information systems?	□ Is your nuclear power facility's operator in compliance with NRC and IAEA cyber security guidelines and consequently implemented information security controls?
□ Does your nuclear power facility use a Supervisory Control and Data Acquisition System (SCADA)?	□ Has your nuclear power facility implemented higher security levels for its SCADA?
□ Does your nuclear power facility have remote access systems?	□ Are remote access systems firewall and password protected?
□ Does your nuclear power facility have an intrusion detection system?	□ Has your nuclear power facility implemented and continuously monitors an intrusion detection system?
□ Does your nuclear power facility separate network segments?	□ Are separate network segments firewall and password protected to prevent access from a less secure segment?

Vulnerability: Transport Hubs

□ Do you fail to take measures to secure air traffic control systems?

□ Do you fail to take measures to secure harbor guidance and control systems?

□ Do you fail to take measures to secure railway marshalling, switching, and signal systems?

□ Do you fail to take measures to secure highway monitoring and control (signaling) systems?

□ Do you fail to take measures to secure nation-wide distribution logistics systems?

Threat: Airports	**Countermeasures**
□ Does your airport use a Flight Data Processing System (FDPS) to manage flight plan related data?	□ Is your facility's FDPS in compliance with the Federal Information Security Management Act?
□ Does your air traffic control facility employ outside IT contractors?	□ Are background checks performed on outside IT contractors?
□ Are air traffic control computers, servers, communications links located in open areas?	□ Are traffic control computers, servers, and communication links located in a secured area with limited physical access?
□ Has the FAA failed to conduct an information systems security assessment of your facility?	□ Are information systems security assessments conducted routinely as part of a greater security management plan?
□ Do specifications for your information systems fail to include security requirements?	□ Do specifications for new or upgraded information systems include security requirements?

Threat: Harbors	**Countermeasures**
□ Does your port facility use a cargo-processing IT system?	□ Is your port facility in compliance with section 15.4.11 of the International Ship and Port Security (ISPS) code that covers IT vulnerabilities?
□ Does your port facility fail to practice information security management?	□ Regarding information security management, is your port in compliance with the industry-accepted international standard, ISO 17799?
□ Does your port utilize a vessel tracking system?	□ Has your port's vessel tracking system been assessed for vulnerabilities?
□ Are your port control facilities located in an open area?	□ Is your port control facility located in a secured area with limited physical access?
□ Has your port failed to conduct vulnerability assessments of its IT resources?	□ Is your port facility in compliance with the Maritime Transportation Security Act (MTSA) of 2002 requiring risk assessment and mitigation?

Threat: Railway Systems	**Countermeasures**
□ Does your railway system use a Supervisory Control and Data Acquisition (SCADA) systems?	□ Has your railway system implemented higher security levels for its SCADA?
□ Does your railway system use wireless connections to maintain communications with trains?	□ Does your railway system encrypt its wireless communications with trains?
□ Does your railway have a train control facility?	□ Is your railway system's train control facility located in a secured, physical-access limited area?
□ Does your railway system use automation and networking in its control facility?	□ Are IT systems and networking in your train control system password and firewall protected and equipped with an intrusion detection system?
□ Does your railway system use a Positive Train Control (PTC) system?	□ Is your railway system's PTC system in compliance with FISMA (Federal Information Security Management Act) and consequently developed a risk-based information security program as well as implementing information security controls?

Vulnerability: Transport Hubs (Continued)

Threat: Highway Systems	**Countermeasures**
□ Is your traffic control and monitoring system automated?	□ Has your automated traffic control and monitoring system been assessed for risks and vulnerabilites?
□ Is your traffic control and monitoring system networked?	□ Are your traffic control and monitoring network password and firewall protected?
□ Does your traffic control and monitoring system use wireless connections?	□ Does your traffic control and monitoring system use encryption for its wireless connections?
□ Does your traffic control and monitoring system use a Supervisory Control and Data Acquisition System (SCADA)?	□ Has your traffic control and monitoring system implemented higher security levels for its SCADA?
□ Does your highway system use a traffic control and monitoring facility?	□ Is your traffic control and monitoring facility located in a secured, physical-access limited area?

Threat: Distribution Logistics	**Countermeasures**
□ Are your distribution logistics reliant on computer networks?	□ Is your distribution logistics network in compliance with FISMA (Federal Information Security Management Act) and consequently developed a risk-based information security program as well as implementing information security controls?
□ Has your distribution logistics network not been assessed for risk and potential harm resulting from unauthorized access and consequent disruption of information systems?	□ Is your database logistics network in compliance with those of the US Armed Forces in times of war and emergency?
□ Does your distribution logistics network fail to have an intrusion detection system?	□ Has your distribution logistics network implemented, and continuously monitors an intrusion detection system?
□ Does your distribution logistics network fail to have backup resources in case of disruption?	□ Has your distribution logistics network implemented a backup plan that includes backup hardware and storage such as servers and communications links in case of disruption?
□ Are your distribution logistics network's servers remotely accessible?	□ Are your distribution logistics network's servers firewall and password protected?

Vulnerability: Internet

- □ Do you fail to take measures to secure physical aspects of your network such as communication links?
- □ Do you fail to take measures to secure Domain Name Servers?
- □ Do you fail to take measures to secure your servers?
- □ Do you lack measures to prevent hacking?
- □ Do you lack measures to mitigate Denial of Service attacks?
- □ Do you fail to take measures to secure your IT assets and networks?
- □ Do you fail to take measures to secure your IT assets and networks against viruses?

Threat: Physical Network	**Countermeasures**
□ Do you have a data center and wiring closets?	□ Do your data center and wiring closets have intrusion alarms that are continuously monitored?
□ Do you have unused network access ports?	□ Are your unused network access ports disabled?
□ Do you have communication cables and harnesses present in your facility?	□ Are communication cables and harnesses placed in such a way to make access difficult for transmission interception?
□ Is your data center located in an open area?	□ Is physical access to your data center restricted by the use of locks, biometrics, or scannable cards?
□ Does your physical network use wireless connections?	□ Are wireless communications strongly encrypted?
□ Do your communications links include fiber optic cables?	□ Are your fiber optic cables placed in such a way to minimize exposure and consequent tampering or damage?

Threat: Domain Name Servers	**Countermeasures**
□ Do you use Domain Name Servers (DNS)?	□ Have you conducted a risk assessment of your DNS servers?
□ Do you fail to install software, patches and upgrades to you DNS operating systems?	□ Do you have a software maintenance plan for installing patches and upgrades to your DNS operating systems?
□ Have you been using the same DNS operating system for 3 to 4 years?	□ Do you regularly install new versions of your DNS operating system as they become available?
□ Do you fail to deploy backup resources for your DNS servers?	
□ Do you fail to restrict traffic to your DNS servers?	□ Do you filter out unnecessary (non-DNS) traffic to your DNS server?
□ Do you allow zone transfers among your DNS servers?	□ Do you disable zone transfers and instead use an encrypted method of transferring zone files from one DNS server to another?
□ Do you use dynamic updates for your DNS maintenance?	□ Do you limit dynamic updates by IP addresses or TSIG (transaction signature) key?

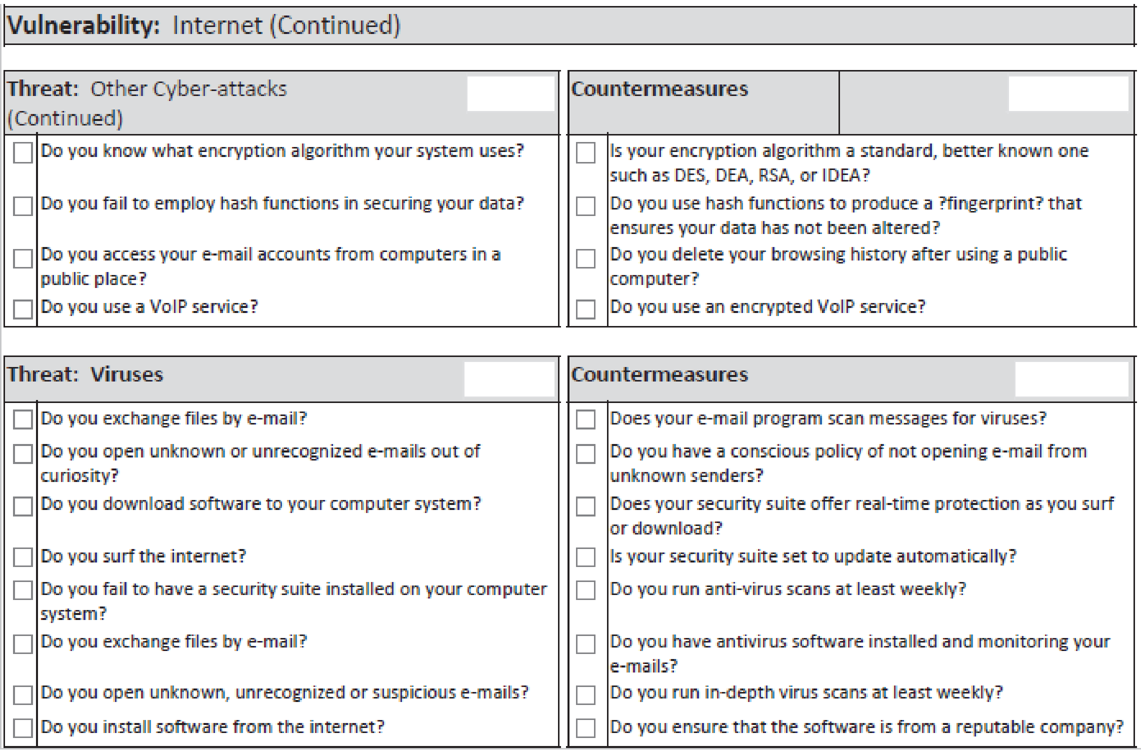
Threat: Other Servers	**Countermeasures**
□ Do you have other servers?	□ Have you conducted a risk assessment of your servers?
□ Do you fail to use password authentication to control access to your servers?	□ Do you have a strong password having special characters, as well as uppercase and lowercase letters to control access to your servers?
□ Do you fail to keep track of who attempts to access your servers?	□ Do you have programs that log and monitor access attempts installed on your servers?
□ Do you fail to install software patches and upgrades to your server operating system?	□ Do you have a software maintenance plan for installing patches and upgrades to your server operating system?
□ Have you been using the same server operating system for 3 to 4 years?	□ Do you regularly install new versions of your server operating system as they become available?

Vulnerability: Internet (Continued)

Threat: Hacking	**Countermeasures**
□ Are your IT systems easily accessible?	□ Do you limit physical access to your IT resources by placing them in monitored, secured areas?
□ Do you have a Static IP address?	□ Do you utilize firewalls and secure routers?
□ Do you have file and print sharing configured on your computer?	□ Do you utilize an intrusion detection system and routinely review the logs?
□ Do you fail to authenticate users?	□ Do you use a password policy for authenticating users?
□ Is your operating system and application software more than 3 to 4 years old?	□ Do you install patches and upgrades to new versions of software as they become available?
□ Do you use forms to accept data from users in a HTTP request?	□ Do you validate data received from an HTTP request before using it in the applications?
□ Do you authenticate users' access to the Web Application?	□ Do you confirm the source of the request before accepting data?
□ Do you use C or C++ code in your application?	□ Do you limit or remove completely all C and C++ code that uses buffers?
□ Does your code use arrays?	□ Does your application test for array size before trying to access the array?
□ Does your application use pointer references?	□ Do you ensure string libraries are implemented correctly in the web application code?

Threat: Denial of Service	**Countermeasures**
□ Do you deploy servers?	□ Do you have a separate emergency block of IP addresses for your servers with a separate route?
□ Do you fail to monitor your IT system performance?	□ Do you have procedures in place to routinely monitor your IT system performance using previously established baselines for typical activity?
□ Do you use routers?	□ Have you implemented router filters designed to prevent SYN flooding?
□ Do you utilize administrative passwords?	□ Have you established a password policy for administrative accounts that uses strong passwords with special characters, uppercase/lowercase combinations, etc.?
□ Do you fail to monitor changes in configuration information?	□ Do you employ tools to detect configuration modifications?
□ Do you fail to review your network services?	□ Do you disable unused or unneeded network services?
□ Do you fail to have redundant hardware and network configuration?	□ Do you have an emergency plan that allows the rapid deployment of backup hardware and network configurations?

Threat: Other Cyber-attacks	**Countermeasures**
□ Have you assessed your IT system risk and potential for harm from unauthorized access and consequent disruption?	□ Have you implemented a risk-based information security program and controls?
□ Is your software more than 3 to 4 years old?	□ Do you regularly install new versions of your software as they become available?
□ Do you fail to install patches and upgrades to your software?	□ Do you have a software maintenance plan for installing patches and upgrades as they become available?
□ Do you fail to monitor your IT system performance?	□ Do you have procedures in place to routinely monitor your IT system performance using previously established baselines for typical activity?
□ Do you fail to have redundant hardware and network configurations?	□ Do you have an emergency plan that allows the rapid deployment of backup hardware and network configurations?
□ Do you utilize administrative passwords?	□ Have you established a password policy for administrative accounts that uses strong passwords with special characters, uppercase/lowercase combinations, etc.?
□ Do you fail to use encryption in your communications?	□ Is your encryption key size 128 bits or higher?



Vulnerability: Internet (Continued)

Threat: Other Cyber-attacks (Continued)	**Countermeasures**
□ Do you know what encryption algorithm your system uses?	□ Is your encryption algorithm a standard, better known one such as DES, DEA, RSA, or IDEA?
□ Do you fail to employ hash functions in securing your data?	□ Do you use hash functions to produce a ?fingerprint? that ensures your data has not been altered?
□ Do you access your e-mail accounts from computers in a public place?	□ Do you delete your browsing history after using a public computer?
□ Do you use a VoIP service?	□ Do you use an encrypted VoIP service?

Threat: Viruses	**Countermeasures**
□ Do you exchange files by e-mail?	□ Does your e-mail program scan messages for viruses?
□ Do you open unknown or unrecognized e-mails out of curiosity?	□ Do you have a conscious policy of not opening e-mail from unknown senders?
□ Do you download software to your computer system?	□ Does your security suite offer real-time protection as you surf or download?
□ Do you surf the internet?	□ Is your security suite set to update automatically?
□ Do you fail to have a security suite installed on your computer system?	□ Do you run anti-virus scans at least weekly?
□ Do you exchange files by e-mail?	□ Do you have antivirus software installed and monitoring your e-mails?
□ Do you open unknown, unrecognized or suspicious e-mails?	□ Do you run in-depth virus scans at least weekly?
□ Do you install software from the internet?	□ Do you ensure that the software is from a reputable company?

Vulnerability: Government Net

□ Is your agency not in compliance with FISMA (Federal Information Security Management Act)?

□ Does your agency fail to have a risk-based information security program?

□ Does your agency fail to implement alert recommendations?

□ Has your agency in the past experienced severe security breaches?

□ Has your agency in the past experienced severe privacy breaches?

Threat: Federal

□ Has your agency failed to stay in compliance with FISMA (Federal Information Security Management Act)?

□ Has your agency failed to implement the EINSTEIN Program?

□ Has your agency failed to implement the Trusted Internet Connections Initiative?

□ Do you fail to receive US-CERT (Computer Emergency Readiness Team) alerts?

□ Do you fail to have redundant hardware and network configurations?

Countermeasures

□ In compliance with FISMA, have you developed a risk-based information security program as well as implementing information security controls?

□ In implementing the EINSTEIN Program, has your agency developed a monitoring system to identify malicious activity and unusual network traffic patterns?

□ As part of the Trusted Internet Connection Initiative, has your agency consolidated the number of external connections?

□ Do you have procedures in place for monitoring and implementing US-CERT alerts?

□ Do you have an emergency plan that allows the rapid deployment of backup hardware and network configurations?

Threat: State

□ Has your agency failed to stay in compliance with FISMA (Federal Information Security Management Act)?

□ Has your state agency failed to receive any US-CERT (Computer Emergency Readiness Team) alerts?

□ Has your state agency failed to monitor its network?

□ Do you fail to have redundant hardware and network configurations?

□ Is your operating system and application software more than 3 to 4 years old?

Countermeasures

□ In compliance with FISMA, have you developed a risk-based information security program as well as implementing information security controls?

□ Does your state agency have procedures in place for monitoring and implementing US-CERT alerts?

□ Has your state agency implemented a monitoring system to identify malicious activity and unusual network traffic patterns?

□ Do you have an emergency plan that allows the rapid deployment of backup hardware and network configurations?

□ Do you have a software maintenance plan that includes installing upgrades and patches as they become available?

Threat: Local

□ Do you fail to have a cyber-security plan?

□ Does your local government fail to receive US-CERT (Computer Emergency Readiness Team) alerts?

□ Does your local government fail to monitor its network?

□ Is your operating system and application software more than 3 to 4 years old?

□ Do your computer systems fail to have a security suite installed?

□ Is your voting machines' software point of origin known?

□ Is the voting machine source code readily accessible?

□ Is the voting machine software routinely scanned for alterations and infections?

□ Is voting data not password or cryptographically protected?

□ Are communications ports and memory card slots easily accessible?

Countermeasures

□ Is your cyber-security plan risk-based and does it feature information security controls?

□ Does your local government have procedures in place for monitoring and implementing US-CERT alerts?

□ Has your local government implemented a monitoring system to identify malicious activity and unusual network traffic patterns?

□ Do you have a software maintenance plan that includes installing upgrades and patches as they become available?

□ Does your security suite offer real time protection and update automatically?

□ Does your voting district verify voting machines' software point of origin?

□ Are safeguards in place to prevent source code access?

□ Does your voting district scan software on a routine basis for alterations and infections?

□ Is voting data protected through the use of passwords and cryptography?

□ Is the ability to access communications ports and memory card slots limited?

Vulnerability: Military Installations

- □ Do you fail to take measures to secure physical aspects of your network such as communication links?
- □ Do you fail to take measures to secure your servers?
- □ Do you fail to take measures to prevent weapons theft/tampering?
- □ Do you fail to take measures to secure unconventional (Nuclear/Biological/Chemical) weapons?

Threat: Physical Network	**Countermeasures**
□ Do you have a data center and wiring closets?	□ Does your data center and wiring closets have an intrusion detection system that is continuously monitored?
□ Do you have unused network access ports?	□ Are your unused network access ports disabled?
□ Do you have communication cables and harnesses present in your facility?	□ Are communication cables and harnesses placed in such a way to make access difficult for transmission interception?
□ Is your data center located in an open area?	□ Is physical access to your data center restricted by the use of locks, biometrics or scannable cards?
□ Does your physical network use wireless connections?	□ Are wireless communications strongly encrypted?
□ Do you rely on satellites for your communications links?	□ Is your satellite communications software point of origin known?
□ Do you have satellite communication hardware present at your facility?	□ Do you limit access to your satellite communication hardware by using fencing, guards, locks, biometrics or scannable cards?

Threat: Servers	**Countermeasures**
□ Do you have servers?	□ Have you conducted a risk-assessment of your servers?
□ Do you have password authentication to control access to your servers?	□ Do you use a strong password having special characters, as well as uppercase and lowercase letters to control access to your servers?
□ Do you keep track of who attempts to access your servers?	□ Do you have programs that log and monitor access attempts installed on your servers?
□ Do you fail to install software patches and upgrades to your server operating system?	□ Do you have a software maintenance plan for installing patches and upgrades to your server operating system?
□ Have you been using the same server operating systems more than 3 to 4 years?	□ Do you regularly install new versions of your server operating system as they become available?

Threat: Weapons Theft/ Tampering	**Countermeasures**
□ Do you fail to take measures to prevent weapons theft/tampering?	□ Does your weapons storage facility have an intrusion detection system that is continuously monitored?
□ Do you fail to control access to your weapons storage facility?	□ Do you have a security plan in place to control access to your weapons storage facility through the use of guards, multiple checkpoints, locks, biometrics and scannable cards?
□ Do you fail to track what is stored in your weapons storage facility?	□ Do you have an inventory tracking system that is continuously updated for your weapons storage facility?
□ Do you fail to have an inspection plan for your weapons storage facility?	□ Are weapons regularly inspected for tampering or damage?
□ Do personnel at your weapons storage facility fail to go through a selection process?	□ Are personnel routinely tested and rotated to avoid complacency?

Threat: Unconventional Weapons	**Countermeasures**
□ Do you have an unconventional weapons (Nuclear/Biological/Chemical) storage facility?	□ Does your unconventional weapons storage facility have an intrusion detection system that is continuously monitored?
□ Do you fail to strictly control access to your unconventional weapons storage facility?	□ Do you have a security plan in place to strictly control access to your unconventional weapons storage facility through the integrated use of guards, multiple checkpoints, locks, biometrics and scannable cards?
□ Do you fail to track what is stored in your unconventional weapons storage facility?	□ Do you have a rigorously adhered to inventory tracking system that is continuously updated for your unconventional weapons storage facility?
□ Do you fail to have a strict inspection plan for your unconventional weapons storage facility?	□ Are unconventional weapons closely and regularly inspected for tampering or damage?
□ Do you fail to use control codes for your unconventional weapons?	□ Are your unconventional weapons control codes strictly guarded and encrypted/password protected?
□ Do personnel at your unconventional weapons storage facility fail to go through a rigorous selection process?	□ Are personnel rigorously screened, psychologically and drug tested, and rotated to avoid complacency?
□ Do you use a computer system for your unconventional weapons deployment and use?	□ Have the computer systems utilized for unconventional weapons deployment and use undergone risk-based vulnerability assessment?

Vulnerability: Financial Net

- □ Do you fail to secure physical aspects of your network such as communications links?
- □ Do you fail to take measures to secure your servers?
- □ Do you fail to back-up and have off-site storage of your data and records?
- □ Do you fail to have a back-up power supply?

Threat: Physical Network	**Countermeasures**
□ Do you have a data center and wiring closets?	□ Does your data center and wiring closets have intrusion alarms that are continuously monitored?
□ Do you have unused network access ports?	□ Are your unused network access ports disabled?
□ Do you have communication cables and harnesses present in your facility?	□ Are communications cables and harnesses placed in such a way to make access difficult for transmission interception?
□ Is your data center located in an open area?	□ Is physical access to your data center restricted by the use of locks, biometrics, or scannable cards?
□ Does your physical network use wireless communications?	□ Are wireless communications strongly encrypted?

Threat: Servers	**Countermeasures**
□ Do you have servers?	□ Have you conducted a risk assessment of your servers?
□ Do you fail to use password authentication to control access to your servers?	□ Do you use a strong password having special characters, as well as uppercase and lowercase letters to control access to your servers?
□ Do you fail to keep track of who attempts to access your servers?	□ Do you have programs that log and monitor access attempts installed on your servers?
□ Do you fail to install software patches and upgrades to your server operating system?	□ Do you have a software maintenance plan for installing patches and upgrades to your server operating system?
□ Have you been using the same server operating system for more than 3 to 4 years?	□ Do you regularly install new versions of your server operating systems as they become available?
□ Do you fail to monitor your IT system performance?	□ Do you have procedures and systems in place to routinely monitor your IT system performance using previously established baselines for typical activity?
□ Do you fail to have redundant hardware and network configurations?	□ Do you have an emergency plan that allows the rapid deployment of back-up hardware and network configurations?

Threat: Data and Records	**Countermeasures**
□ Has your organization failed to comply with the Sarbanes-Oxley Act?	□ Is your Sarbanes-Oxley compliance record keeping and document management software secured through electronic signatures, passwords, and the use of non-editable formats?
□ Are your data and records stored at one facility?	□ Is your data and records storage redundant and dispersed in case of catastrophe at one site?
□ Do you use the internet to access data and records?	□ Does your IT system feature routers, firewalls, installed security suites, as well as password authentication?
□ Do you store your data and records on servers?	□ Have you conducted a risk assessment of your servers?
□ Do you fail to back-up your data and records?	□ Does your organization have strictly adhered to procedures for backing up data and records to multiple storage locations?

Threat: Power Supply	**Countermeasures**
□ Do you rely on the power grid for electricity?	□ Does your facility have a back-up generator?
□ Are power outages common in your area?	□ Does your IT hardware have UPSs (Uninterruptible Power Supply)?
□ Do you fail to have redundancy built into your system?	□ In case of outage, can you shift operations to unaffected facilities?
□ Have you failed to plan for disruption?	□ In case of disruptions, do you have an emergency plan that has been rehearsed and is familiar to personnel?
□ Are power substations in your area easily accessible?	□ Has your utility made efforts to secure power substations by locating them underground or fencing them off?

Vulnerability: Health Institutions

□ Do you fail to take measures to secure physical aspects of your networks such as communication links?

□ Do you fail to back-up and have off-site storage of your data and records?

□ Do you fail to take measures to secure your servers?

□ Do you fail to take measures to secure your Nuclear/Biological/Chemical agents and drugs?

Threat: Physical Network	**Countermeasures**
□ Do you have a data center and wiring closets?	□ Do your data center and wiring closets have intrusion alarms that are continuously monitored?
□ Do you have unused network access ports?	□ Are your unused network access ports disabled?
□ Do you have communication cables and harnesses present in your facility?	□ Are communication cables and harnesses placed in such a way to make access difficult for transmission interception?
□ Is your data center located in an open area?	□ Is physical access to your data center restricted by the use of locks, biometrics, or scannable cards?
□ Does your physical network use wireless connections?	□ Are wireless communications strongly encrypted?
□ Do your communications links include fiber optic cables?	□ Are your fiber optic cables placed in such a way to minimize exposure and consequent tampering and damage?

Threat: Servers	**Countermeasures**
□ Do you have servers?	□ Have you conducted a risk assessment of your servers?
□ Do you fail to use password authentication to control access to your servers?	□ Do you use a strong password having special characters, as well as uppercase and lowercase letters to control access to your servers?
□ Do you fail to keep track of who attempts to access your servers?	□ Do you have programs that log and monitor access attempts installed on your servers?
□ Do you fail to install software patches and upgrades to your server operating system?	□ Do you have a software maintenance plan for installing patches and upgrades to your server operating system?
□ Have you been using the same server operating system for more than 3 to 4 years?	□ Do you regularly install new versions of your server operating system as they become available?
□ Do you fail to monitor your IT system performance?	□ Do you have procedures and systems in place to routinely monitor your IT system performance using previously established baselines for typical activity?
□ Do you fail to have redundant hardware and network configurations?	□ Do you have an emergency plan that allows the rapid deployment of back-up hardware and network configurations?

Threat: Data and Records	**Countermeasures**
□ Has your organization failed to comply with the Sarbanes-Oxley Act?	□ Is your Sarbanes-Oxley compliance record keeping and document management software secured through electronic signatures, passwords, and the use of non-editable formats?
□ Are your data and records stored at one facility?	□ Is your data and records storage redundant and dispersed in case of catastrophe at one site?
□ Do you use the internet to access data and records?	□ Does your IT system feature routers, firewalls, installed security suites, as well as password authentication?
□ Do you store your data and records on servers?	□ Have you conducted a risk assessment of your servers?
□ Do you fail to back-up your data and records?	□ Does your organization have strictly adhered to procedures for backing up data and records to multiple storage locations?

Threat: Nuclear/Bio/Chem Agents	**Countermeasures**
□ Do you have Nuclear/Bio/Chem Agents and drugs present at your facility?	□ Have you conducted a risk assessment of Nuclear/Bio/Chem agents and drugs present at your facility?
□ Do you lack software and procedures for keeping track of your inventory of these agents and drugs?	□ Do you have software and procedures in place for thoroughly tracking the location, use, and disposition of these agents and drugs in your facility?
□ Do you fail to limit access to these agents and drugs?	□ Is physical access to these agents and drugs tightly controlled through the use of locks, guards, biometrics, scannable cards and personnel authorization policies?
□ Do you fail to store these agents and drugs securely?	□ Does the storage facility for these agents and drugs have an intrusion alarm system that is continuously monitored?
□ Do you fail to screen personnel handling these agents and drugs?	□ Are personnel authorized to handle these agents and drugs closely screened using background checks, drug and psychological testing?

Vulnerability: Water Supply/Food Chain

□ Do you lack back-up and off-site storage of your data and records?
□ Do you lack funding and staffing for your inspection and testing facility?
□ Do you fail to limit physical access to your facilities?
□ Do you fail to take measures to secure your Nuclear/Biological/Chemical agents?

Threat: Data and Records	**Countermeasures**
□ Is your organization required to comply with the Sarbanes-Oxley Act?	□ Is your Sarbanes-Oxley compliance record keeping and document management software secured through electronic signatures, passwords, and the use of non-editable formats?
□ Are your data and records stored at one facility?	□ Is your data and records storage redundant and dispersed in case of catastrophe at one site?
□ Do you use the internet to access data and records?	□ Does your IT system feature routers, firewalls, installed security suites, as well as password authentication?
□ Do you store your data and records on servers?	□ Have you conducted a risk assessment of your servers?
□ Do you fail to back-up your data and records?	□ Does your organization have strictly adhered to procedures for backing up data and records to multiple storage locations?
□ Do you fail to maintain chain-of-possession record keeping?	□ Does your organization utilize chain-of-possession record keeping so that all persons handling items such as chemicals and foodstuff are known?

Threat: Inspection and Testing Facilities	**Countermeasures**
□ Does your inspection and testing facility lack adequate funding and staffing to properly carry out its mission?	□ Has your inspection and testing facility secured all the funding available to it through governmental and corporate sources ?
□ Is your inspection facility not in compliance with FDA and EPA regulations?	□ Does your inspection and testing facility routinely review newly released FDA and EPA regulations for implementation and compliance?
□ Has your inspection and testing facility failed to implement industry best practices?	□ Does your inspection and testing facility review scientific and trade publications for implementation of the latest industry best practices?
□ Does your facility fail to keep up with the latest hardware and software advances for inspection and testing?	□ Does your facility seek out and purchase the latest inspection and testing hardware and software?
□ Do you fail to protect the computers used for processing inspection and test data?	□ Do the computers used for the processing of inspection and test data have firewalls and security suites set up to do weekly anti-malware scans?

Threat: Physical Access	**Countermeasures**
□ Do you fail to limit access to reservoirs and water retention pools?	□ Do you limit access to reservoirs and water retention pools through the use of locked perimeter fencing and guards?
□ Do you lack measures for securing access to water treatment facilities?	□ Do you have measures in place at your water treatment facility to secure access by using locked perimeter fencing, guards, biometrics, scannable cards and personnel authorization policies?
□ Do you fail to limit access to foodstuff storage and processing areas?	□ Do you limit access to foodstuff storage and processing areas by the use of locked perimeter fencing, guards, biometrics, scannable cards and personnel authorization policies?
□ Do you fail to make your food packaging tamper-proof?	□ Do your food packaging processes result in tamper-proof products?
□ Do you fail to screen personnel with access to your facilities?	□ Do you have procedures in place to screen and test personnel with access to your facilities by using background checks, drug and psychological testing?

Threat: Nuclear/Bio/Chem Agents	**Countermeasures**
□ Do you have Nuclear/Bio/Chem agents present at your facility?	□ Have you conducted a risk assessment of the Nuclear/Bio/Chem agents present at your facility?
□ Do you lack software and procedures for keeping track of these agents?	□ Do you have software and procedures in place for thoroughly tracking the location, use, and disposition of these agents in your facility?
□ Do you fail to limit access to these agents?	□ Is physical access to these agents tightly controlled through the use of locks, guards, biometrics, scannable cards, and personnel authorization policies?
□ Do you fail to store these agents securely?	□ Does the storage facility for these agents have an intrusion alarm system that is continuously monitored?
□ Do you fail to screen personnel handling these agents ?	□ Are personnel authorized to handle these agents closely screened using background checks, drug and psychological testing?

About the Authors:

Dr. M. Sahinoglu is the founding Director of the Informatics Institute and Head, Cybersystems and Information Security Graduate Program at Auburn University at Montgomery (AUM). Formerly, the Eminent Scholar and Chair-Professor at Troy University's Computer Science Department,he holds a B.S. and M.S. in Electrical and Computer Engineering, and Ph.D. in EE and Statistics jointly. He conducts research in Cyber-Risk Informatics.He is the author of Trustworthy Computing (2007) and Cyber-Risk Informatics: Metric Evaluation (2014).

Chris Kelsoe, Major USAF, is on active duty with Maxwell AFB in Montgomery and is soon to be graduating from AUM's CSIS program with a Master's degree.

Scott Morton is a part-time research associate at AUM and adjunct instructor at Troy University Montgomery campus. He holds a M.S. in Computer Science from Troy University Montgomery and a B.A. in International Relations from Johns Hopkins University.

Dr. Meltem Eryilmaz is a faculty member in Computer Engineering Department at Ankara's ATILIM University. She holds a B.S. in Statistical Science, M.S. in Computer Engineering, Ph.D. in Cyber Education and Instructional Technology. She conducts research in Adaptive, Blended and Flip learning and recently in the Cybersecurity Risk Management domain. She worked as a Training Specialist at Microsoft Training Center, Software Channel Manager at Microsoft VA Distributor and Managing Director at Oracle VA Distributor from 1994 to 2001.