IA R-US Support to GIAC Enterprises

GIAC Enterprises:

Global Intravenous Appliance Conglomerate (GIAC) Enterprises is a new small pharmaceutical supply Firm, providing hospitals, clinics, and offices with equipment for blood and saline delivery. All Plant operations and warehousing is conducted on-site in Key Largo, FL. Operations continue for 16 hours each day, 5 days a week. GIAC Enterprises runs 2 shifts of production crews from 05:00 a.m. until 9:00 p.m. Administrative staff operate between 8:00 and 5:00 p.m.

The corporate Information Technology (IT) department is known as the Systems Office. This department provides IT and Management Information Systems to support administrative issues, such as payroll, benefits, internal and external electronic correspondence, Internet access, orders receipt, financials, product inventories and audit production and health of manufacturing equipment. Complete loss of the main IT systems would result in inability to continue operations, during the downtime. The IT Systems Office is responsible for a risk management effort to be conducted in support of corporate networks. IT Systems has a technician on staff 24 hours a day, seven days a week. Full staffing is available during normal business working hours, matching the administrative staff.

Information Assurance Resources – United States (IA R-US):

IA R-US is composed of 10 Information Assurance practitioners from the military and Government consulting firms who came together to create a specialized consulting group and capture US Government business. Besides the Human Resources partner, who acts as office manager, the remaining initial nine employees are all highly skilled in different facets of Information Assurance and general networking. The “billable 9” possess multiple current certifications from the SANS institute, (ISC)^2, ISACA, CISCO systems, and MicroSoft Corporation. A technical writer/editor is sub-contracted to proof-read written deliverables prior to final draft.

When first established, the 10 partners of IA R-US created a Mission Statement that identified the business base and targeted customer base.

IA R-US provides the highest quality of information assurance consulting services to our customers centering on Government organizations through detailed research, quality analysis, and expertly prepared deliverables.

Part 1: Methodology and Process

Request for Proposal:

GIAC Enterprises submitted a short request for proposals (RFP) in an information assurance trade magazine. The following RFP was submitted:

GIAC Enterprises Systems Office (GESO) Information Assurance (IA) program is a critical program to support our growing business base and is required for most of the other key technology programs in GESO. Consequently, validating our security posture is high priority (important) and urgent. GESO seeks experienced Information Assurance risk management support services to perform a detailed risk assessment on our corporate network to validate and verify our security posture.

The purpose of the Information Assurance effort is to create the basis of confidence in our corporate security. Our IA architecture must be capable of withstanding system stresses from insider and outside threat agents through adaptive and robust protection and management of information and information transport services. It must further verify our effectiveness regarding our proactive defenses, our detective measures, and our ability to respond and recover from incident. Interested parties must be able to provide all of the following services: 1) conduct a comprehensive Information Technology Risk Assessment with distinct but integrated Communications and Information Systems components, 2) identify assets, threats, and vulnerabilities that might impact the confidentiality, integrity and/or availability of GIAC Enterprises assets, and 3) provide risk reduction countermeasures based upon the vulnerabilities identified in the risk analysis. Demonstrated prior performance is a qualifying factor; therefore, certification of prior successful risk assessment performance and two current or previous client references must be provided to qualify.

Proposals sought are for thorough risk assessment methodology and performance capability. Proposals shall not exceed 10 pages, font Arial, 12 pitch, single-spaced, Cost proposals shall be not more than 1 of the 10 pages, the remaining are for understanding and technical approach to the RFP requirements including the management plan. Corporate qualifications and personnel biographical pages may take up not more than 2 additional pages. Use of graphics and color are recommended, where justified. All submissions must include Company Name, Contact Person Name, Address, Telephone Number, and Fax Number. Submissions must be provided to GIAC Enterprises, ATTN: GESO, at or before 1700 on Friday, 11 June 2004. Proposals may be faxed to (813) 555-1111. Proposals shall be reviewed and ranked for award based upon passing technical approach, demonstrated capability and then cost. Bidder’s conference will be held at GIAC Enterprises Corporate Headquarters on Friday, May 14th. The point of contact is Mr. George Jetson at (813) 555-1212 or e-mail: george.jetson@giacent.com.

During the bidder's conference, it was determined that personal qualification would suffice for the client references, rather than requiring such performance to have been as "IA R-US". For the fledgling IA R-US organization, this was important to qualify under the terms of the RFP.

It was known that GIAC Enterprises was serious about the quality of the contract award. Therefore, to ensure that nothing was forgotten in their short RFP statement of work, the exact statement of work was used as a baseline to respond with IA R-US understanding, before moving on to the risk assessment a and management approaches. Once it was determined IA R-US personnel were considered qualified to submit based on extensive personal IA experience by the "billable 9", the following proposal was built and forwarded to GIAC Enterprises. While the team had mostly government experience, they decided to push on their strengths. This proposal was built on four win-themes:

Win-Themes:

- Extensive Personnel IA Experience
- Team players – Team Solidarity
- Solidly formulated detailed risk assessment methodology built on Government protection requirements
- Extensive Risk Management knowledge (If page-count limit remains - work in additional related capabilities (contingency planning, ST&E, etc)).

PART 2

Information Assurance Resources – United States Proposal For Global Intravenous Appliance Conglomerate Enterprises

Executive Customer:

Global Intravenous Appliance Conglomerate (GIAC) Enterprises is a new small pharmaceutical supply Firm, providing hospitals, clinics, and offices with equipment for blood and saline delivery. Their Systems Office Director has initiated a Request for Proposals (RFP) to support the need to validate the security of their network for key corporate stakeholders. Information Assurance Resources – United States (IA R-US) is pleased to provide the Director the following understanding and technical approach, as well as information regarding other services that compliment the risk assessment called for in the RFP.

Understanding of Requirements

The GESO IA program is crucial to the corporate growing business base. Therefore, GESO must immediately contract expertise to validate the corporate security posture. GESO requires Information Assurance experts from IA R-US to provide risk management support services and perform a detailed risk assessment on the GIAC Enterprises corporate network to validate and verify the corporate Microsoft/Intel-based network IA security posture.

Absence of appropriate risk management will result in a potential inability to communicate with administrative and corporate support systems within GIAC Enterprises. Therefore, accreditation without proper analysis and countermeasure implementation will put the Chief Executive Officer and board of directors at undue legal risk. The Chief Executive Officer must be made aware of the risks to the corporate systems through the conduct of a formal risk assessment, and potentially subsequently tasked security test and evaluations, Additionally, development of system security plans, security operating procedures, and contingency plans.

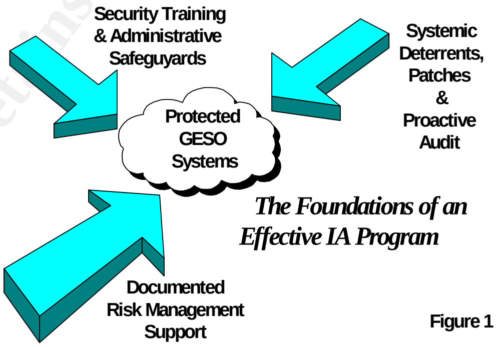

Security Training & Administrative Safeguards
Systemic Deterrents, Patches & Proactive Audit
Protected GESO Systems
The Foundations of an Effective IA Program
Documented Risk Management Support

Figure 1

Our highly-sedulous IA R-US Team must unquestionably verify for GIAC Enterprises that the IA architecture must be capable of withstanding system stresses from both insider and outside threat agents by validating the adaptive and robust protection capabilities and inherent management of information and information transport services. IA R-US must further verify our effectiveness regarding our proactive defenses, our detective measures, and our ability to respond and recover from incident. GESO requires IA R-US to conduct a comprehensive Information Technology Risk Assessment of the GIAC Enterprises network. In doing so, IA R-US must identify the network assets, identify threats that may impact those assets, identify in-place countermeasures that exist to reduce impact through vulnerability mitigation, and to identify and additional vulnerabilities that increase risk to GIAC Enterprises and their shareholders. In addition, GIAC Enterprises requires IA R-US to analyze identified vulnerabilities and provide risk reduction countermeasures that will reduce the risk posed by those vulnerabilities to an acceptable level.

When considering IA, technical personnel often look singularly to the data, and are under the misguided mind-set that sophisticated systemic security features are adequate to protect GIAC Enterprises system assets. Technical security features are useful for the cases of data confidentiality and integrity. However, there are other resource integrity and availability issues that cannot be supported by systemic features. They are not responsible for user security awareness. They are not responsible for painting the entire picture for the Chief Executive Officer, board of directors, or shareholders, or putting together the appropriate paperwork. IA R-USD is interested in helping provide the best possible IA program. Nonetheless, the responsibility, and the effectiveness of the program, now rest singularly with GIAC Enterprises.

GIAC Enterprises selection of IT-RUS on this contract will ensure top-qualified expert performance of the required risk assessment effort, ensuring that any subsequent State or Federal information system assets and that inspection and audit teams are impressed with our progress. Our team is composed of experienced practitioners that have, and still may, hit the process running, rather than having to learn the various levels of requirements from the customer or an expedient crash course.

Roles

GESO will be the customer and point of contact. They are also interviewees, being the customer. Based on the Bidder's Conference input, GESO will perform periodic reviews of the risk assessment progress as per their desires, not to exceed one review a month, and not to delay work more than 3 business days of review.

IA R-US will provide all analysis services. Our team will conduct interviews, perform required research and analysis, and document the risk assessment deliverable.

Because IA R-US and the identified IA R-US offices and staff are located in Miami, we are in a prime position to exercise their experience in ensuring that the IA program to support GIAC Enterprises plant operations in Key Largo, Florida.

Proposed Support Approach

Project Management

This effort shall be managed by our Corporate President, Mr. Rob Ashworth. We will provide continual weekly status update verbally with the Director of GESO, or his delegate throughout the effort. We will provide written reports on a monthly basis, delivered not later than the 5th of the following month. Our bid is firm-fixed price, therefore, no financial status information will be necessary. Mr. Ashworth will personally supervise this effort and all personnel, assigning tasks until product delivery.

Risk Assessment Methodology

Our team will conduct the network-level risk assessment in any required format. However, our personnel have decades of experience working risk management for the U.S. Government, including work on classified systems, the protection of which ensures continued freedom in our Country. Our standard methodology is one that has grown by our team when supporting the Department of the Navy. It is based upon OPNAVINST 5239.1A Method II Risk Assessments that provide a detailed look at complex systems and networks, with the weighting factors and threat factors from a methodology used by former Defense Information Systems Agency and Immigration and Naturalization Service (when it existed). Our methodology provides a highly detailed look at network assets, potential threats that might impact those assets, and the vulnerabilities that might cause a threat to occur, resulting in harm to or effectiveness reduction of information system assets; then quantify the cost of countermeasures to mitigate the risks. Our team members, combined, can boast the accomplishment of over 50 such risk assessments, on complex systems and networks. If, for some reason, GIAC Enterprises requires the conduct of a more detailed old-style Method I type (FIPS Publication) Risk Assessment, our team contains experienced members or leaders of these teams, as well. Our experience with many complex methodologies enhance our analytical capabilities and the value of our proposed Risk Assessment format. We accomplish the risk assessment in 7 phases as follows:

Stage 1: Establish the Effort:
In this step, we begin by identification f the customer, which has been accomplished as the Director of GIAC Enterprises Systems Office. We will next define the system, identifying the extent of the system and at what internal or external port on what router or other network device the GIAC Enterprises control and the extent of the effort end. Next, we identify the RA team members. This includes not only the IA R-US personnel, but also critical GIAC Enterprises personnel with whom we will working closely in this IA effort. Preliminary introductions and interviews are then conducted at the end of Stage 1.

Stage 2: Identify and Quantify Assets
In reality, this stage overlaps Stage 3. These are data-gathering phases including review of existing policy, laws, system and network documentation, network architecture and system configurations. Protective systems employed will be closely analyzed, to include router access lists, and how these lists and any firewall tables are configured. Account default and group permissions will be analyzed. In addition, service pack and patch implementation status will also be reviewed against GIAC Enterprises testing process to ensure that security patches are installed in a timely manner. When gathering data for assets and threats, we keep in mind to never double-count any asset, but to identify and quantify all assets. Once assets are identified and quantified for corporate loss purposes, we analyze all four impact categories (modification, destruction, disclosure, and denial-of-service) and then look to the worst-case category for documentation purposes.

Stage 3: Meanwhile, we also start to identify Threats that might impact system assets. We look at threats such as natural disaster threats (e.g., hurricanes, tornadoes, floods, electrical storms, earthquakes), human action threats (e.g., aircraft crash, unauthorized physical access, unauthorized network access, misuse of computer resources, unauthorized disclosure, unauthorized user action), and other threat categories (e.g., interference, compromising emanations, etc). Once we have established the threats, we analyze them against network safeguards to determine what safeguards are in-place to mitigate risk, and document them. We then look at potential vulnerabilities to our assets through threat exploitation of the vulnerabilities that are not protected well enough by in-place countermeasures, and document them. Other concerns or comments are also documented that are not considered a vulnerability or safeguard. Throughout, We will ensure that any requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 are carefully addressed.

Stage 4: We determine risk levels at this stage. IA R-US uses a 5-level end rating for each threat-to-asset pair, as opposed to the standard stoplight 3-level approach. Our rating levels and their descriptions are provided below:

REMOTE – This assessment is made when the threat is considered: (a) extremely unlikely to occur based on the existing safeguards and history, and/or (b) to have relatively insignificant detrimental impact on that asset if it does occur. No further countermeasures are required.

LOW – This assessment is made when the threat is considered: (1) unlikely to occur based on adequate controlling safeguards and history, and/or (2) to have a little detrimental impact on that asset if it does occur. Attention may be considered for low-cost risk reduction.

MODERATE – The risk of a given threat to a specific asset is assessed as being possible or having a notable impact in causing harm to and/or reducing the effectiveness of that asset as a result of destruction, modification, disclosure of data, or denial of service to that asset. Concern is warranted.

HIGH – The risk of a given threat to a specific asset is assessed as having a potentially significant impact on that asset as a result of destruction, modification, disclosure of data, or denial of service. This analysis is made when the threat is considered to have a reasonable potential of occurrence and, upon such occurrence, will result in significant impact on that asset. Extreme concern is warranted, additional countermeasure application is recommended.

SEVERE – This analysis rating is made when the threat is considered to have an extreme likelihood of occurrence and, will result in a catastrophic impact on that asset. Immediate countermeasure action is warranted.

NOT APPLICABLE – The threat does not apply to the asset under evaluation.

Stage 5: Determine and justify Recommended additional countermeasures.

At this time, we document additional recommended countermeasures to mitigate vulnerabilities that have resulted in unsatisfactory risk ratings. All proposed countermeasures are evaluated to determine their effectiveness in reducing the potential impact of existing vulnerabilities. Each proposed additional countermeasure is evaluated on a stand-alone basis to allow the GESO Director to implement any combination of the proposed countermeasures individually. Because this risk assessment is not fully quantitative in nature, return on investment (ROI) calculations are not performed. Please note that identified countermeasure costs are estimated, and may vary upon implementation.

Stage 6: Complete Introduction & Executive Summary

When Preparing the risk assessment document, once it is complete and further technical editing is not required, the introduction is completed and the executive summary written. The location of this stage in the process allows us to ensure that modifications that might impact the executive summary and introduction are all made prior to this stage, so that those sections will be valid against the overall document.

Stage 7: Final Edit & Delivery

When the technical team has completed their portion, they work with a syntax editor to ensure the quality of the document, while making sure that the intent of all statements of fact within the assessment do not change the meaning intent. When completed, we print and bind 3 copies, with soft copies on disk, and provide these to our customers. We will deliver the required risk assessment in 3 copies of quality-bound hard-copy format, each containing a CD-R with the risk assessment in soft-copy format, using "Microsoft Word" word processor. All corporate proprietary documentation that was released to IA R-US is also returned.

ADDITIONAL SERVICES THAT MAY BE REQUESTED BY GESO

Security Test & Evaluations

Security Test & Evaluation methodologies include abbreviated and comprehensive types. Abbreviated methods mimic the checklist-type risk assessment methodologies, and can be conducted by any experienced IA practitioners. However, personnel who are experienced in development of comprehensive ST&Es are few. Our experienced resources have led or otherwise been part of the development and execution of over a dozen of these test plans for complex systems and networks, including mainframe systems, and various local and wide area network configurations. They have played integral roles in the development and execution of comprehensive ST&Es for mission-critical complex systems of various classifications for organizations such as The Naval War College, USSOCOM, US Forces Command, and SPAWAR.

We will designate a development team composed of expert resources, and turn test plans over to GIAC Enterprises for review, approval, and subsequent execution. We will ensure that some members of our team are available to support the execution. The execution support personnel, who were not on the Risk Assessment or ST&E development teams, will then document the results, to remove test-result biases.

Contingency Plans

System Contingency Plans must be system-specific and comprehensive, taking into account all levels of contingency, from loss of access to certain system devices or applications for short periods, to complete destruction of system assets. For complex systems, they can become very detailed. Data sensitivity levels, hardware and software configurations, location of the user-base, and location of a designated hot, cold or alternate (warm) site are necessary. They must also be tested and updated, in some fashion, at least annually. Our team is experienced with working with system administration personnel, primary users, and application functional managers to qualify the data into levels of criticality. Then, to research and identify alternate methods of ensuring the primary user-base can resume the minimum survivability-level of operations within their specified maximum downtime. Once all potential loss factors have been researched, procedures will be documented and key individuals informed about their role under the various loss scenarios. Once the plan, and the procedures to implement the plan, are developed, accepted by the user-base and GIAC Enterprises, testing scenarios will then be established and implemented on an annual basis, after functional management and GIAC Enterprises approval. Any problems with the contingency plan procedures during testing will be documented, and the plan updated.

Information Systems Security Policy

IA R-USD has been placed on a contract as a sub-contractor to develop security policy for the Space and Naval Warfare Command (SPAWAR) Headquarters' Information Assurance Manager's organization. Currently, the IA R-US President is responsible for publication of SPAWAR and SPAWAR Systems Center Charleston IT policy and standards. IA R-US personnel have also, under other Firms, supported the conduct of activity-wide accreditations, including the drafting of activity-level 5239-series instructions, for dozens of IAMs/ISSMs throughout the Department of the Navy and various Joint Service DoD activities, such as Department of Justice, Department of Homeland Defense, USCENTCOM, USSOCOM, USASOC, Naval Special Warfare Group 1, Naval Special Warfare Command, and SPAWAR Systems Center, San Diego. In the past half year, our team has drafted two Navy 5239-series instructions and two small policy statements in support of the IA program at SPAWAR for the Department of the Navy. Our team has the experience, and understanding of existing and emerging Federal laws and Regulatory policies to continue to support any future policy writing requirements for GIAC Enterprises through our extensive Government support experience. We will review the pertinent senior guidance for exact reference citations and develop the policy in support of regulatory laws and as directed by GIAC Enterprises security officials, should you wish to add this tasking.

IA Training

Our team developed the current one-hour IA Awareness Users training class based on a requirement from the NISE East training department, while IA R-US accepted the responsibility of initiating the IA program. There exists a fervent requirement to educate the IA Personnel regularly. This training must be in much greater detail than the User Awareness training. Network Security Managers must understand their function in supporting the overall program. Members of our team have developed entire NSM-level curriculums for various agencies, and are active members of the Federal Information Systems Security Educators Association. Using our combined experience, our team will develop a sophisticated training course, including detailed lesson plan, computer-generated graphics, and practical applications to practice performing risk assessments based on applicable Regulatory guidance as approved by GIAC Enterprises. We will develop a similar class in developing ST&E test plans, and any other required areas, as tasked by GIAC Enterprises.

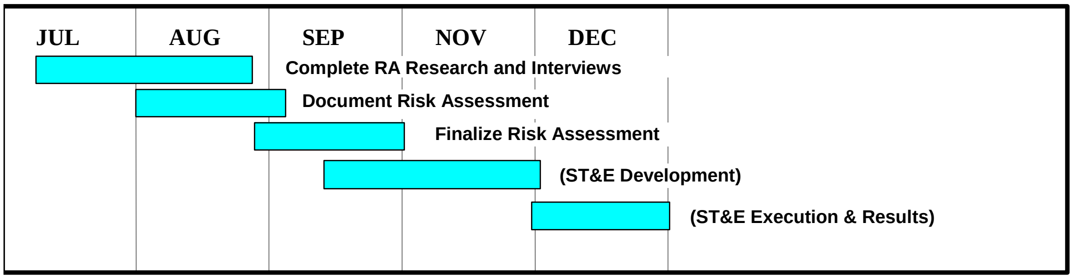
Proposed Schedule

Figure 3 below provides a proposed schedule of events for our risk analysis team. This schedule is subject to change based on the needs of GIAC Enterprises and their requirements of the various overall capabilities presented in this document. Provided as an example, this schedule identifies key requirements that may be completed by the team outlined in the first estimate, and additionally, if GESO desires, the completion of a detailed ST&E.

Cost Proposal:

This Cost Proposal is submitted as a Full-Fixed Price proposal, based on the requirements and completion of our methodology for one network risk assessment and analysis. Our four expert analysts will be employed for an accelerated discounted commercial rate of $100 per hour. This rate provides an average of their General & Administrative costs, salaries, benefits, and profit.

It is estimated that this risk analysis will require approximately 3/4 staff-year, or 1500 hours to research, interview, inspect, analyze, document and review our risk assessment deliverable. In addition, Travel and Material requirements are estimated at an actual cost plus standard load. This results in an estimated total fixed-price cost of $150,000.



Qualifications

IA R-US is a new organization composed of Information Assurance and Risk Management professionals. Our lack of corporate qualifications is negated by our extensive personnel qualifications, which are adequate as per Mr. Jetson's response at the Bidder's Conference. Personnel Qualification Biographical for the 4-person key team proposed to support GESO's requirement are summarized in the table below and highlights are summarized in the following paragraphs:

Mandatory Requirements	Analyst Team	Technical Team
Risk Assessments	High	Moderate
Comprehensive ST&Es	High	Moderate
Sec. Operating Procs	High	High
Security Training	High	Low
Ad-Hoc Support	Moderate	Moderate
Firewall & System Security Tech Admin.	Low	High

Table 1.

Table 1 identifies essential system-level IA functional service requirements, including some not required in this RFP, that IA R-US can easily support., and how much input the analysis and technical teams use in interaction to support the overall program. C

Team Members	Program Management	Security Design	Information Mgmt. System	Administrative Support	Risk Assessment	Configuration Management	Training	SOPs	Security Analysis	Full ST&E's	Survey	Contingency Plan	Activity Policy	DoD Clearance
Rob Ashworth	▦	≋	▦	≋	▦	▦	≋	≋	≋	▦	▦	▦	▦	🔴
Barney Rubble		≋	▨	▦	▦	≋	▨	≋	≋	≋	▨	▨	▨	🟡
Fred Flintstone	≋	≋	≋	▨	▦	▨	⁞	⁞	⁞	▨	▨			🟡
Homer Simpson		▨	▨	▨	▦	⁞	⁞	▨	⁞	▨	▨	⁞	⁞	🟡

⁞ <1 year
▨ 1 - 4 years
≋ 4 - 8 years
▦ 8+ years
🔴 Top Secret
🟡 Secret
🔵 Confidential

Table 2.

Table 2 lists primary accreditation support and technical support personnel and their experience levels. This table provides a team with combined skills that are not otherwise available from a "one-stop" supply in our geographical region. The combined experience of recognized experts in the different facets of IA, the key areas that GIAC Enterprises may require both currently and in the future, are all available within a single local organization - IA R-US.

Robert C. Ashworth, M.S.I.A., B.A., “Professor-of-Practice” for Network Security, Capitol College. President, Information Assurance Resources – United States, Inc. (IA R-US). Mr. Ashworth is an employee and founder of IA R-US where he currently provides Information Assurance (IA)/Information Systems Security and Program Management services to Marine Forces – Atlantic and SPAWAR Headquarters IA Manger’s office. He also provides I.T. policy and information systems security consulting services for other clients, primarily U.S. Government. Previous I.A. management positions over the past decade have been with Price-Waterhouse Coopers L.L.P. and Booz-Allen and Hamilton. Mr. Ashworth possesses the two core Information Systems Security-related certifications from (ISC)², “Certified Information Systems Security Professional (CISSP)” and “Systems Security Certified Practitioner (SSCP).” He also possesses the SANS Institute GIAC Certified Incident Handling Analyst (GCIH) as well as and Certified Intrusion Analyst (GCIA) certification, the GIAC Security Essentials certification (GSEC) and previously held the GIAC Windows Security (GCWN) certification. Professor Ashworth now also holds the new CISM certification from ISACA, and is also a member of the SANS GIAC GCIH and Security Awareness Advisory boards.

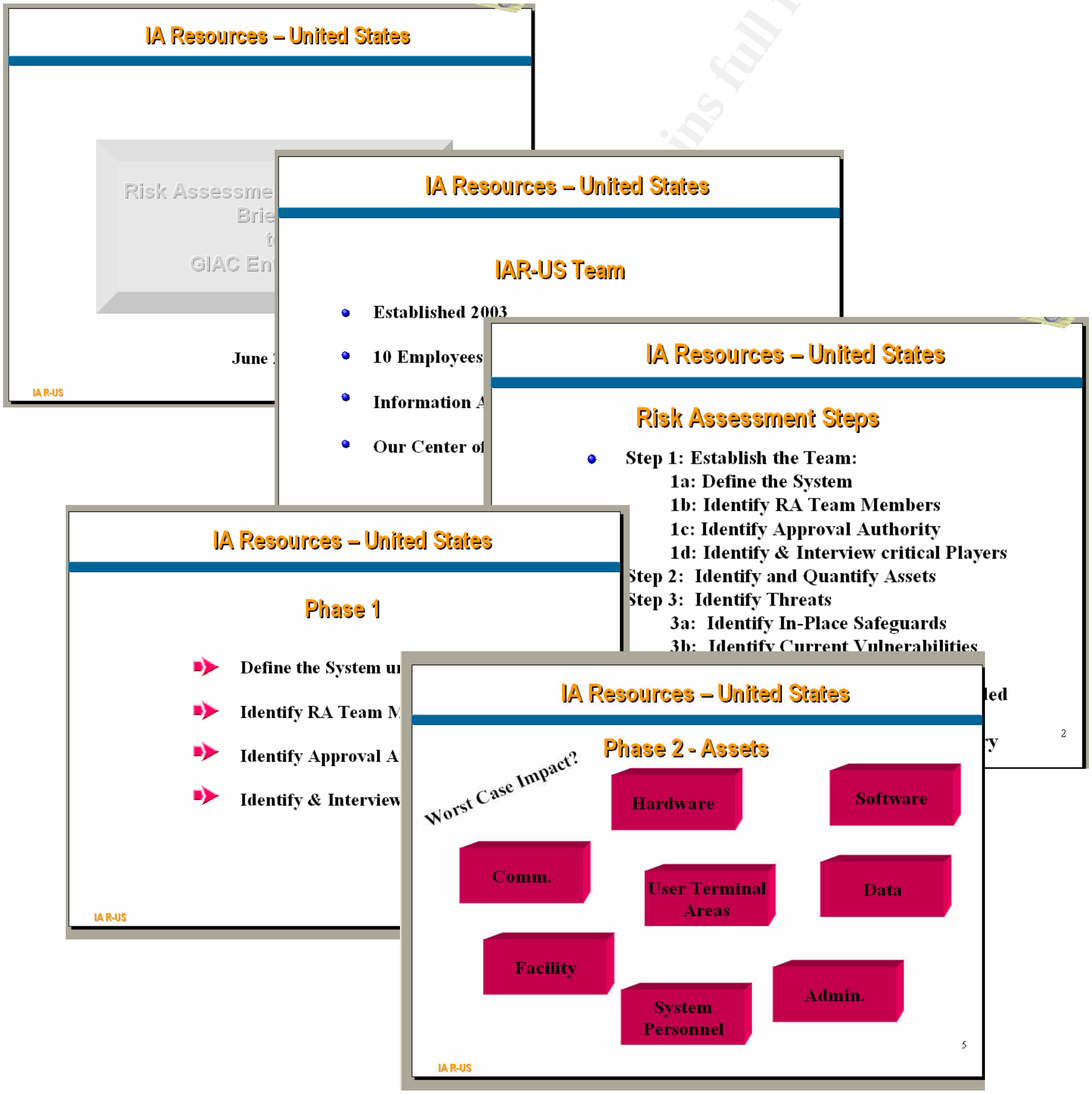
Fred D. Flintsone, B.S. LtCol Flintstone, Vice President – Risk Management Projects, IA R-US. Mr. Flintstone is a Retired Lieutenant Colonel, USMC. Subequent to 22 years of work in the Information Assurance field for the Marine Corps and Joint Commands, he was released from Active duty in October 2003 having served is final duty as the Chief of Information Assurance and Information Assurance Manager (a.k.a ISSM) for US Central Command’s Information Technology Directorate (J-6). Mr. Flintstone possesses the CISSP, Cisco Certified Network Associate (CCNA), GCIH, and GSEC certifications.

Barney B. Rubble, MSBA, B.S. – Computer Science. Associate, IA R-US. Mr. Rubble has 5 years of experience subsequent to obtaining his Master’s degree from Duke University. He has been working on tasks in support of Department of Justice and the banking industry for SAIC, Inc., prior to transferring to IA R-US. His experiences for DoJ include risk assessment and ST&E test plan research and development, and the development of a wireless security policy, as well as user security SOPs. Mr. Rubble is certified as GCWN and GSEC from the SANS Institute.

Homer Simpson – B.S. – Network Security. Homer is new to the work-force, but is centering his attention on medical, pharmaceutical, and HIPPA security requirements. He has a bachelor’s degree, graduating Cum Laude, in Network Security from Capitol College, MD. While there, during work/study, he assisted in many of the campus security efforts, including development of many of their technical policies and SOPs. Homer possesses an interim Secret clearance. Homer received and “A” in his Risk Management course that is relevant to this effort – and is currently pursuing the SANS Institute GSEC certification.

The Pitch.

While the proposal is submitted on schedule ad dictated by the request for proposals and the bidders' conference, an oral pitch to ensure that GIAC Enterprises is ensured of the quality of the personnel was recommended during the bidder's conference. Therefore, Mr. Ashworth scheduled an appointment to meet with Mr. Flintstone and others from GIAC Enterprises and their Systems Office. The exact team proposed for the effort were scheduled to proceed to GAIC Enterprises to conduct a methodology briefing. The briefing provided capabilities information, but was centered upon our team risk assessment methodology, to win this effort and get IA R-US's foot in the door of GIAC Enterprises.



IA Resources – United States

Risk Assessme
Brie
t
GIAC En

June

IA R-US

IA Resources – United States

IAR-US Team

- Established 2003
- 10 Employees
- Information A
- Our Center of

IA Resources – United States

Risk Assessment Steps

- Step 1: Establish the Team:
  1a: Define the System
  1b: Identify RA Team Members
  1c: Identify Approval Authority
  1d: Identify & Interview critical Players
  Step 2: Identify and Quantify Assets
  Step 3: Identify Threats
  3a: Identify In-Place Safeguards
  3b: Identify Current Vulnerabilities

led

ry

2

IA Resources – United States

Phase 1

- Define the System u
- Identify RA Team M
- Identify Approval A
- Identify & Interview

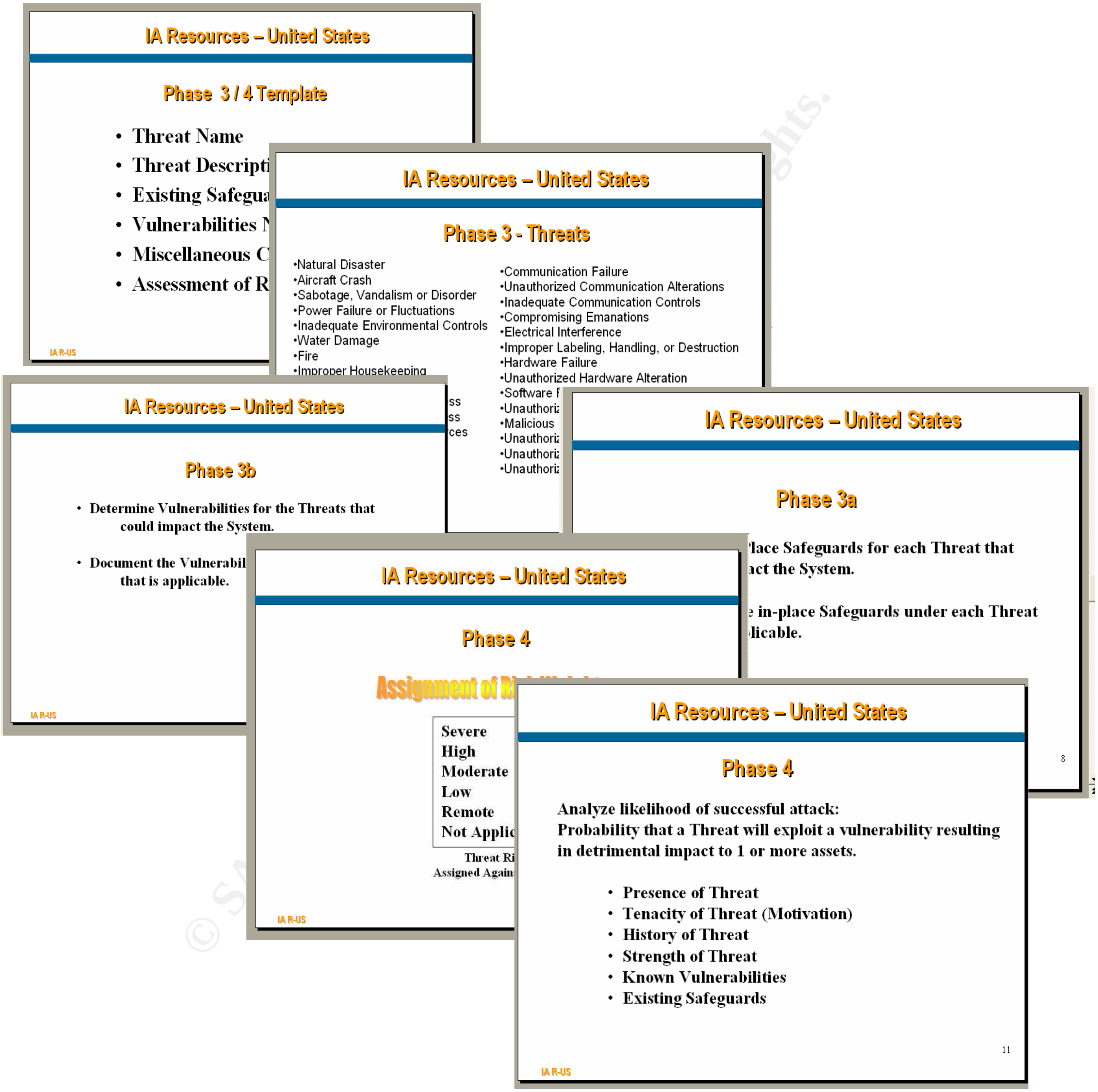
IA R-US

IA Resources – United States

Phase 2 - Assets

5

IA R-US



IA Resources – United States

Phase 3 / 4 Template

- Threat Name
- Threat Descripti
- Existing Safegua
- Vulnerabilities N
- Miscellaneous C
- Assessment of R

IA R-US

IA Resources – United States

Phase 3 - Threats

•Natural Disaster
•Aircraft Crash
•Sabotage, Vandalism or Disorder
•Power Failure or Fluctuations
•Inadequate Environmental Controls
•Water Damage
•Fire
•Improper Housekeeping
ss
ss
ces

•Communication Failure
•Unauthorized Communication Alterations
•Inadequate Communication Controls
•Compromising Emanations
•Electrical Interference
•Improper Labeling, Handling, or Destruction
•Hardware Failure
•Unauthorized Hardware Alteration
•Software F
•Unauthoriz
•Malicious
•Unauthoriz
•Unauthoriz
•Unauthoriz

IA Resources – United States

Phase 3b

- Determine Vulnerabilities for the Threats that could impact the System.
- Document the Vulnerabil that is applicable.

IA R-US

IA Resources – United States

Phase 3a

lace Safeguards for each Threat that act the System.

e in-place Safeguards under each Threat licable.

8

IA Resources – United States

Phase 4

Assignment of Ri

Severe
High
Moderate
Low
Remote
Not Applic

Threat Ri
Assigned Again

IA R-US

IA Resources – United States

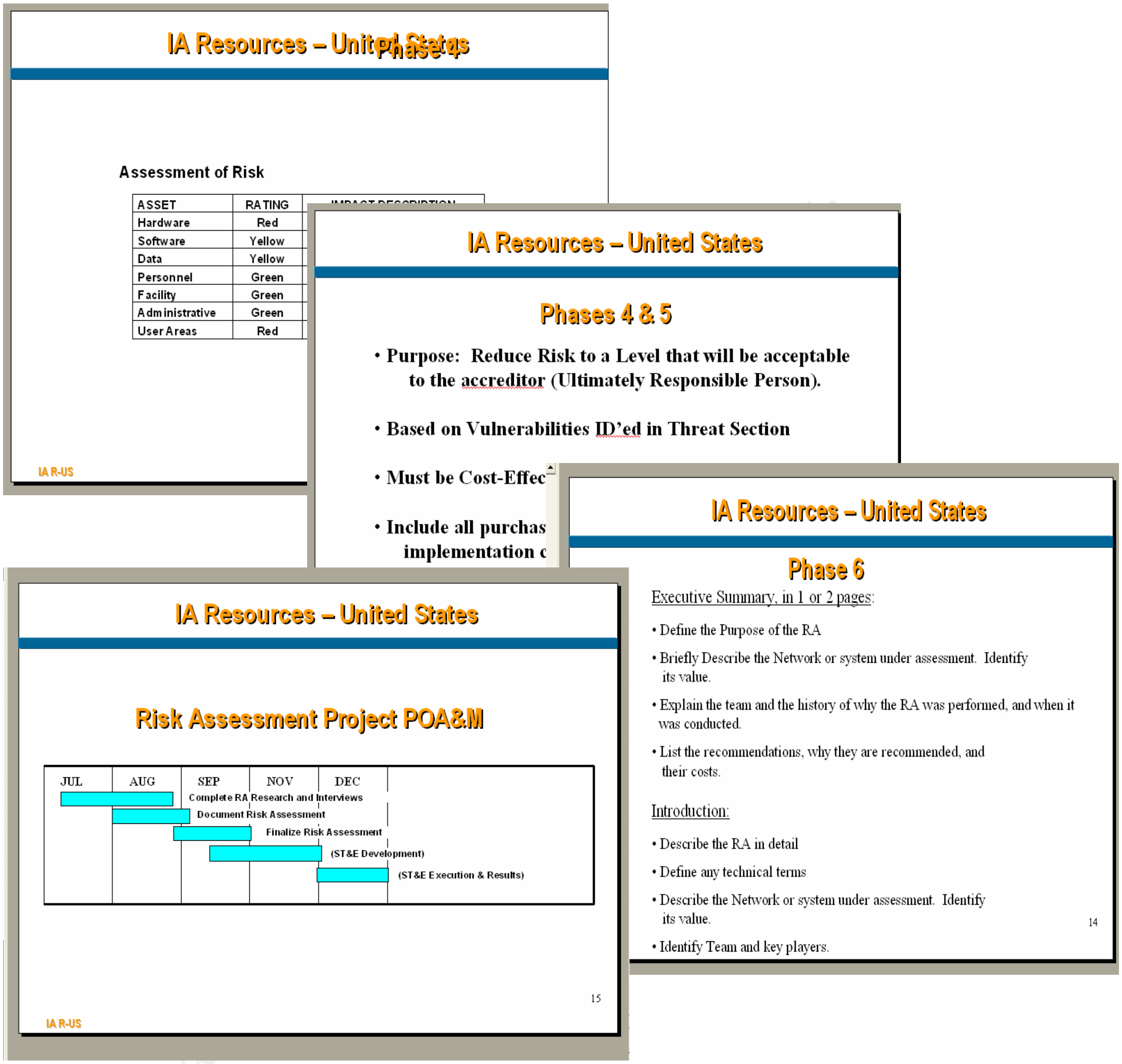
Phase 4

Analyze likelihood of successful attack:
Probability that a Threat will exploit a vulnerability resulting in detrimental impact to 1 or more assets.

- Presence of Threat
- Tenacity of Threat (Motivation)
- History of Threat
- Strength of Threat
- Known Vulnerabilities
- Existing Safeguards

11

IA R-US



IA Resources – United States
Phase 4

Assessment of Risk

ASSET	RATING	IMPACT DESCRIPTION
Hardware	Red	
Software	Yellow	
Data	Yellow	
Personnel	Green	
Facility	Green	
Administrative	Green	
User Areas	Red	

IA R-US

IA Resources – United States

Phases 4 & 5

- Purpose: Reduce Risk to a Level that will be acceptable to the accreditor (Ultimately Responsible Person).
- Based on Vulnerabilities ID'ed in Threat Section
- Must be Cost-Effec
- Include all purchas implementation c

IA Resources – United States

Phase 6

Executive Summary, in 1 or 2 pages:

- Define the Purpose of the RA
- Briefly Describe the Network or system under assessment. Identify its value.
- Explain the team and the history of why the RA was performed, and when it was conducted.
- List the recommendations, why they are recommended, and their costs.

Introduction:

- Describe the RA in detail
- Define any technical terms
- Describe the Network or system under assessment. Identify its value.
- Identify Team and key players.

14

IA Resources – United States

Risk Assessment Project POA&M

15

IA R-US

Part 3

Memorandum

From: Rob Ashworth, President, IA R-US
To: Fred Flintstone, Barney Rubble, Homer Simpson
Cc: All-staff group

Subject: Project Plan

As was announced yesterday afternoon, IA R-US has been awarded the risk assessment effort at GIAC Enterprises in Key Largo, FL. (Company celebration details to follow).

The effort start date, and first billable date, is designated as Tuesday, July 6th. Labor Charge number will be GIACEN-100001-003-2004. Travel and Materials charge number will be GIACEN-100002-003-2004. Charge questions should be directed to me. Full time employees to bill to this effort are on the “to” line of this memorandum. We will be commuting. You are encouraged to car-pool, but may drive independently at 40 cents per mile, no more than 50 mile charged, each way. This is considered local travel, so meals are on your dime. If any of you need to exceed 12 paid trips to the client-site, you must get my approval.

Please note that I have agreed, upon their request as part of our “Best and Final Offer”, to reduce the effort form 3 to 2 months. This is a very aggressive schedule, but also doable!

The following schedule and plan of action is directed:

Phase 1: July 6th @ 0800 – Company Conference Room: Kick-off meeting. Mr. Jetson from GIAC Enterprises is scheduled to join us at 1000, Ms. Cogswell will be picking him up in the morning for lunch and our questions and answers. He will be bringing corporate policies and network architecture diagrams with him. We will pour over those policies and plans over the rest of the week.

Phase 2: July 12th @ 0900 - Our RA team will meet Mr. Jetson at GIAC Enterprises for a tour and identification of our key points-of-contact. After lunch, our data gathering will begin in earnest with Phase 2 data gathering of asset information.

Fred: You will be responsible to get with their IT Production folks and get hardware and software cost figures for existing infrastructure. You will gather and complete hardware and software asset information. Assume Destruction to be the worst-case impact category. You should have a draft by the end of the week. Consider IT communications to be under the hardware and software asset categories.

Barney – You'll have to get with IT management and production management to get a handle on data and it's value. We need to determine their backup and contingency operations plans. Learn what you can to determine the worst case impact – could be destruction or disclosure… possibly even modification if a competitor wished to sabotage them. While there, gather administrative asset data. Drafts are due on Friday the 16th.

Homer – I want you to scan Tuesday for unauthorized wireless access points. Also, get with facilities and start gathering physical information regarding the building reconstruction, A/C upgrades, fire-suppression, floor stress, all of that. Work with Barney or me on format – it's due Friday the 16th. I will center my attention on user areas and the terminal assets.

When you go on-site, I want you all to commute down there. It's about 50 miles from this office, so I'll use that as a local-travel cost basis, though I know some of you live closer. I expect you on-the-job there for 7 good/solid hours on the client site each day. We haven't yet been awarded follow-on work, but we did pitch it in our proposal, and some of the other staff are short on billability. Every Friday, regardless of the week, we will meet at 0800 to 0900 in the company conference room, here at IA R-US to provide discussion on our status. I will be providing a summary to GIAC Enterprises later in the day, each Friday.

While you are gathering asset information, start considering the threats.

Stage 3: During the week of July 19th, we'll begin to lock in on our threat-specific interviews.

Fred, with your background and the asset's you're covering, I want you to start looking closely at in-place safeguards and vulnerabilities for the threats of:

- Sabotage, Vandalism or Disorder
- Power Failure or Fluctuations
- Inadequate Environmental Controls
- Communication Failure
- Unauthorized Communication Alterations
- Hardware Failure
- Unauthorized Hardware Alteration
- Software Failure
- Unauthorized Software

Barney, please coordinate with Fred, as some safeguards and vulnerabilities will cross over between threat categories that you 2, and Homer, are covering. With your experience, you will be responsible for the threats of:

- Misuse of Computer Resources
- Unauthorized Network Access
- Electrical Interference

- Improper Labeling, Handling, or Destruction
- Malicious Software Infestation
- Unauthorized User Action

Homer, we'll try to help you, and start you out with ones that require some interviews of the local police, fire department, as well as the site security and other support function personnel. Many of your threats will overlap with Sabotage, Vandalism, and Civil Disorder, se be sure to coordinate with Fred, as well as Barney. Your responsibilities are completion of threats of:

- Natural Disaster
- Fire
- Theft
- Water Damage
- Improper Housekeeping
- Aircraft Crash
- Unauthorized Physical Access
- Unauthorized Disclosure

Upon the completion of the 2nd week on-site, we shouldn't need to be commuting each day. I will want you to use the week of July 26th to put together a solid draft document of your sections for my review, which I'll do the weekend of July 31.

Stage 3 (Continued) The week of August 2, you will get together to incorporate my comments and finalize your data still outstanding with the customer. I'll have to complete the monthly report and deliver it before August 5th. You'll all work together to "one-voice" your input and combine it all to make a single document, which I'll review over the weekend of August 7th. I'll also need Ms. Cogswell to start working up the graphics for the binder covers, spines, CD-R covers, and tables of contents. I'll want to review the art work by August 20th.

Stages 4 and 5: The week of August 9th, I want you to finalize your risk ratings and once I approve each one, write the recommended additional countermeasures to reduce risk through vulnerability mitigation. They should be const-effective solutions. This will be the end of your effort. Make sure that you have EVERYTHING you need from the customer by the close of this week!

Stage 6: During the week of August 16th, we'll finish the introduction and Executive Summary and then one-voice and syntax edit the document. I've sub-contracted Barney's wife, Mrs. Betty Rubble, for the task – a former middle-school grammar teacher, she is very accomplished! Barney, I'll need you to work side-by-side with her to ensure that no syntax edits change the meaning of what the author intended.

Stage 7: I'll perform a final review on the 23rd and we'll work any modifications in on the 24th. I want 3 copies created and soft copies as well on the 25th for delivery on the 27th. That gives us a full day for error and to complete our August monthly report. Hopefully, coming in ahead of their compressed schedule will help them come to us for follow-on work!

Very Respectfully, Rob

Budget:

IA R-US will have a 100K budget at loaded/accelerated rate for the actual work on this. Our office manager will also be charging from a separate program management slice of the actual award.
Award: $140,000 (Cost reduced during "Best and Final Offer" shoot-out).
Profit/Business Development: $15,000
Office/Program Management labor: $10,000
Facilities & Equipment: $15,000
Travel: $.40 x 100 miles x 12 trips x 4 cars = $1,920.
Materials: $80 is budgeted for consumable materials.
Telephone Charges and cellular phone bills: Part of the PM set-aside.
Syntax Editor Sub-contractor: Negotiated "2 pass" review flat-rate cost of $5,000.
This leaves a budget of $93,000 toward project labor.

Anticipated project labor charges are as follows:

	Loaded Rate	Hours	
Rob Ashworth	$110.00	260	$28,600.00
Fred Flintstone	$100.00	260	$26,000.00
Barney Rubble	$85.00	260	$22,100.00
Homer Simpson	$60.00	260	$15,600.00
		TOTAL:	$92,300.00

Communication Requirements:

Rob Ashworth will provide a Friday afternoon status meeting, each week, with the customer, in the manner as required by the customer. In addition, a written monthly status report will be provided before the 5th calendar day of August summarizing July work, and with the final delivery at the end of August. No report format was specified in the statement of work, so we will create a detailed summary of monthly project happenings to ensure that the customer is a fan of our efforts. Should there be any mishap or other complaint, the Director of GESO has Rob Ashworth's personal cellular number, as well as the numbers of all others on the team and the main IA R-US office number.

Meeting/Interview Felicitation – Part 3: Partial Interview Questionnaire:

Memorandum

From: Rob Ashworth, President, IA R-US
To: Homer Simpson
Cc: Fred Flintstone, Barney Rubble,

Subject: Project Data Gathering Questionnaire

I've pasted below a partial questionnaire that I plan to use to get the overall document started, only 15 questions of my initial battery. Please take a look and comment.

Respectfully, Rob

GESO Director or IT Manager:

1. Provide a description and frequency of data file back-up?

2. Who determines which files are backed-up?

3. Where is the back-up media stored?

4. How are new users granted access to the system and who determines access privileges?

5. Is access to individual's data files restricted to approved users? If yes, what mechanism enforces the restrictions?

6. How are removable magnetic media controlled from unauthorized entry or exit from GIAC Enterprises facilities?

7. Describe how passwords are generated and distributed to users.

Facilities and/or Security Manager:

8. Are there documented procedures on what to do when an individual is no longer allowed access to the facility and/or system?

9. Are unauthorized personnel or visitors allowed in the facility and have escort procedures been documented?

10. How do you restrict unauthorized computer facility access?

11. What processes and mechanisms do you use to protect against and combat malicious software?

12. Have there been power failures in the area that have affected your computer operations?

13. GIAC Enterprises is in a heavily hurricane-prevalent area – what measure do you have in place for protection of the facility and assets?

14. GIAC Enterprises is in a tropical area, please identify the output capabilities of your air conditioning, backup air conditioning against heat output of the equipment.

15. Is an Uninterrupted Power Supply (UPS) provided to the computer system? If yes, what are its components and replacement cost: Is there a maintenance contract on the UPS? What type of contract and at what cost?

Potential Pitfalls – Part 3:

There are many issues that can come up that can cause problems to such an effort.

a) Hurricane Activity. To cut costs and thus increase profits, I'm requiring my personnel to commute to the client location, which is exactly 47.2 miles by road from our headquarters location. This effort is occurring during Hurricane Season in Key Largo, and we have a drop-dead date for completion. Problems due to natural disaster for our completion were not provided in the contract, so we are legally liable to complete the effort.

   Our Plan: We will keep abreast of tropical waves and storms moving from Africa to ensure we have warning. When a hurricane-level tropical storm is likely to strike the Keys or Miami, 2-days out, we will ensure we gather whatever we can work on remotely from the client site at that time. I have secured working spaces for emergency operations in Raleigh, NC. The four-person key-team will use extra PM funds to relocate there and work on what we have, verifying additional information via telephone for as long as we can. Should the hurricane shift North, we will wait until it passes the Florida area and return to South Florida to resume operations.

b) Scope Creep. The customer compressed the timeframe and through the Best and Final Offer process, was able to reduce the expenditure fort he deliverable an additional $10,000. Scope creep can continue should the customer ask that additional work be accomplished over and above the terms of the contract within the existing funding and timeframe agreement.

   Our Plan: To allow our President, Rob Ashworth to provide summary reports to them each Friday, and to continue dialogue that will allow him to keep good relations while diplomatically identifying any potential additional requests for further work and respond with such comments as "Would love to! Shall I send a cost estimate for that additional work to you, or to someone else?" or other response to keep both parties in keeping with the contract and to allow only those requests that he deems to be in the best interests of the Firm.

Value Add – Part 3:

Memorandum

From: Rob Ashworth
To: Fred Flintstone, Barney Rubble
Cc: Homer Simpson

Subject: Value Added

1. As you know, I have always subscribed to Ken Blanchard's "*Raving Fans*" method of conducting business, and one of his principles is to provide 101% to the customer, because a satisfied customer is not enough… we want "Raving Fans". Therefore, a couple recommended additional countermeasures have come to my attention that will permit us to provide additional valuable information to GIAC Enterprises without much additional work on our part.

2. It appears that some of the weaknesses we have encountered thus far include lack of standard security operating procedures and lack of a contingency plan. We have at our disposal examples of these types of documents. I propose that after identifying the recommended additional countermeasures for at least he contingency plan, that we include a detailed outline, or very detailed tables of contents. This (these) outlines should be tweaked from some of our best available examples toward GIAC Enterprise's specific needs, rather than just pasting in canned solutions.

3. I feel that providing a template or two to them in phase 5 of our risk assessment will be value added to our risk assessment deliverable and aid them in filling in the meat, and may actually end up with them asking us to do the development under additional tasking and funding!   Our proposal did mention our capabilities in these areas. Fred – Please ensure that this happens before my review, so that I can comment on this/these templates, as well.

4. During the delivery presentation, I plan to recommend that they have an ST&E performed as well. We also noted our expertise in this area, in our proposal.

   Best Regards,

   Rob

RISK ASSESSMENT

FOR THE

KEY LARGO FACILITY
GIAC ENTERPRISES
SYSTEMS OFFICE
CORPORATE
LOCAL AREA NETWORK

GIAC Enterprises
Key Largo Facility
1775 GIAC Lane
Key Largo, FL 12345-6789

AUGUST 2004

DELIVERABLE
Part 4 – Section A

EXECUTIVE SUMMARY

Risk is the combination of the likelihood that an unwanted event will take place with the impact that the event will cause. A solid risk management analysis of a computer network considers all factors that can cause harm to or reduce the effectiveness of all or a portion of the network assets. Therefore, to determine risk, a risk assessment is made to consider all threats that might impact network assets within the following areas of concern:

- Confidentiality: Ensuring that data is not disclosed to unauthorized individuals.
- Integrity: Ensuring that the network assets remain intact, and in operational mission readiness, as intended.
- Availability: Ensuring that network assets are provided as intended, when authorized users need access.

This risk assessment was performed on the GIAC Enterprises Systems Office (GESO) Corporate LAN environment from 1 through 25 August 2004. It was conducted to provide a qualitative analysis of the GESO Corporate LAN AIS security posture. Using a combination of the best features from established Government methodologies as a base, the quantitative measures were modified to weighted factors in the manner derived from a U.S. Government format. The GESO Director may use documentation contained in this report to assist in determining acceptable operations and to justify additional countermeasure procurement in support of Corporate LAN operations.

The GESO Corporate LAN functions primarily as an administrative LAN to the GIAC Enterprises and subordinate Companies and all elements of the Key Largo Facility for GIAC Enterprises that provides GIAC Enterprises with administrative and support electronic operations as well as Internet access. It provides mission-critical automation capability to GIAC Enterprises' Key Largo Facility. Site personnel stated the highest category of data processed or stored in the system is proprietary sensitive.

The Risk Assessment Team identified and valued all network and end user computing equipment assets. Each asset value was determined based on possible loss according to the worst case impact category (modification, destruction, disclosure, and/or denial of service) per occurrence. Each asset loss value was calculated for that asset without alone to adequately consider the total loss of each asset without the possibility of double-counting portions of the values. The total value to the GIAC Enterprises of all assets is estimated to be $4,106,388. Twenty-two general threat categories were evaluated to determine the probability of successful attack against the identified assets.

An analysis of the threats reveals that the most serious issues requiring management attention are vulnerabilities within the three threats of *Sabotage/Vandalism/Civil Disorder/Terrorism, Misuse of Network Resources* and *Fire.* The vulnerabilities related to these threats are cause for great concern and may have an impact on the mission accomplishment of the GESO Corporate LAN in the future.

Twenty additional countermeasures are proposed for implementation and are listed below. Details are provided in Section 5 of the full document. Implementing these countermeasures will significantly reduce the risk of operating the GESO Corporate LAN. The mandatory and recommended countermeasures are listed below in order based on estimated return on investment.

- Document Contingency Plan and Procedures.
- Review Audit Trail
- Provide Security Training to GESO Staff
- Modify Automatic Enable of Lock-out Feature
- Develop Standard Security Operating Procedures
- Install Water Detection Devices
- Implement Automatic Time-out Feature
- Establish Off-site Storage for Backups
- Dail-in Access Security.
- Install Internet-Capable Anti-Virus Software.
- Procure and Maintain Backup Network Servers
- Maintain Accurate Equipment Inventory for Network and End-User Equipment
- Restrict Internet Access to Official Uses Only
- Physically Secure Communications Closets
- Install Shunt Trip in GESO
- Implement Fire Awareness Program
- Implement Fire Prevention Inspection Program
- Inspect and Correct Overheating in Communications Closets
- Label All Emergency Switching Devices
- Implement Manual Visitor Auditing

GIAC Enterprises Management should review the cost-effectiveness of these countermeasures, with respect to the availability of financial and personnel resources or other constraints, and make a formal determination on implementing the countermeasures. Sections of this report contain additional in-depth information regarding noted deficiencies.

TABLE OF CONTENTS

Section 1

INTRODUCTION

A risk assessment evaluates Automated Information System (AIS) assets, threats, and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. A risk assessment determines if existing countermeasures are adequate to reduce the probability of loss to an acceptable level and determines the need for additional cost-effective countermeasures. To analyze the GIAC Enterprises Systems Office (GESO) Corporate Local Area Network (LAN), the risk assessment team used their decades of Government information assurance risk management experience to create a thorough risk assessment methodology based on a combination of different Government risk assessment methodologies to create the best combination method for a comprehensive outcome.

An overview of procedures used in conducting each major step of the methodology is contained in the key sections of this risk assessment report. The appendices provide additional information in support of the initial four sections. Average GIAC executive, plant workers and corporate office workers rates were used within each pay grade, based on the actual average of the user community in these three areas. Labor rates used represent unburdened (i.e., non-accelerated) actual labor rates. The risk assessment data gathering and documentation effort was performed jointly during an aggressively scheduled short-term effort by computer security specialists from IA R-US during 1 through 25 August 2004. Additionally, various local technical experts provided essential input to the development and wholeness of this analysis.

RISK ASSESSMENT TEAM

NAME	ORGANIZATION
Robert Ashworth	Information Assurance Resources - US
Fred Flintstone	112233 TechAlley Way
Barney Rubble	Miami FL, 55512
Homer Simpson	

LOCAL TECHNICAL EXPERTS

Mr. Hootie Blowfish	NSO - Network Operations Center
Ms. Sandra Bullock	GIAC Enterprises Security Manager
Mr. Clint Eastwood	Channel 4 Meteorologist
Capt. Clark Kent	Key Largo Police Department
Chief Tom Horne	Key Largo Fire Department
Mr. Joe Rotorhead	Key Largo Airport Air Operations
Mr. Harvey Wallbanger	GIAC Enterprises Facilities
Mr. Steve Wonder	GESO Network Security Manager
Mr. George Jetson	GIAC Enterprises Systems Office

Section 2

INFORMATION SYSTEMS SECURITY ENVIRONMENT PROFILE

A synopsis of the GESO Corporate LAN environment located at GIAC Enterprises Plant, Key Largo Facility, FL is provided in the following paragraphs.

1. Hardware - Hardware supporting the GESO Corporate LAN consists of 3 servers, 2 communications backbone hubs, 3 routers (2 owned by the Network Operations Center, Quantico), 1 front end processor with channel extender and T-1 Internet connection through AT&T, 14 CD ROM drives, 10 modems, and various end user computing equipment (approximately 700 desktop workstations/laptops, 280 printers, and 62 scanners). The wiring within the GESO GIAC Plant is Gigabit fiber optic between the closets (one redundant link per wire closet) with CAT5 100KBit drops to the users. Other equipment supporting the Corporate LAN include cables, uninterrupted power supply, etc.

2. Data - Data stored on the GESO Corporate LAN is all proprietary sensitive information. It consists of official correspondence, internal memorandums, E-mail messages to local and remote site personnel, financial planning spreadsheets, procurement documents, and various other documents in support of administrative functions.

3. User areas - There are various user areas connected to the GESO Corporate LAN which are located in the Key Largo Facility perimeter. The majority of the GESO Corporate LAN workstations are Pentium-4 IBM-compatible personal computers with various printers and scanners supporting users at the desktop.

4. Software - Network applications supporting office automation include Lotus Smartsuite (5.0) and Microsoft Office 2002. The primary operating system is Microsoft Windows 2000. Email tools is via Microsoft Exchange. Time management is supported by MS Outlook/Exchange 2002 and MS Project. Dial-in software is MS Remote Access Server, and the antivirus protection software is currently McAfee Anti-Virus and Symantec Corporate Edition AntiVirus.

5. Personnel – All GESO personnel are considered essential to the sustained the availability and functionality of the GESO Corporate LAN in support of the user community.

6. Facility - The GESO Corporate LAN facility is 500 square feet of converted office space. These spaces include air conditioning, preaction dry-pipe sprinkler, and raised flooring upgrades. Personnel and user office spaces are not considered essential assets of the GESO Corporate LAN; therefore, are not considered under the auspices of this Risk Assessment.

7. Administrative - Vendor-supplied manuals are available to support GESO Corporate LAN personnel to operate, maintain, and troubleshoot the network. Supplies include NIC cards, communication cables, spare components, and consumables.

Section 3

ASSET DESCRIPTION WORKSHEETS

Eight assets were addressed for the GESO Corporate LAN: hardware, communications, data, software, personnel, facility, administrative, and user areas. To determine realistic dollar amounts for applicable ways in which threats can affect assets, an evaluation was conducted to determine the effect of the most significant impact. The possible impacts considered were modification, destruction, disclosure, and denial of service. These scenarios and assumptions are documented on the Asset Identification and Valuation Worksheets. At the request of GIAC Enterprises, Plant Production Equipment, whether connected to corporate networks or not, were not considered an asset category under this risk assessment.

The assets identified for the GESO Corporate LAN and associated dollar values are:

Hardware/Comm ....………....	$3,413,988
Data ....…….........	100,000
Software ....…….......	146,700
Personnel ....…….........	320,000
Facility ....…….........	75,000
Administrative ....…….........	125,625
User Area(s) ....……….............	983,500
Total Assets	$4,106,388

Unless otherwise noted, the impact category of destruction is considered the worst case in valuing assets. Dollar values used in the valuation process represent site-unique cost factors as closely as possible. These representations are assessed in light of existing, in-place countermeasures. The impact areas are:

Modification: Cost to detect, locate, and correct the modification. This includes permanent loss of use of a portion, but not all, of particular asset, or temporary loss of use of the entire asset.

Destruction: Market replacement costs for complete loss of an asset based on the replacement costs as opposed to original asset costs and any associated denial of service resulting from that asset loss.

Disclosure: Assigned dollar values for intentional or unintentional disclosure of proprietary sensitive data.

Denial of Service: Cost incurred and any penalties assessed because of delay in work completion. Calculations for average users including GIAC corporate office workers, Plant workers and civil servants were not based on accelerated (i.e., burdened) labor rates.

HARDWARE ASSET IDENTIFICATION AND VALUATION WORKSHEET
(Includes Communication Assets)

Description	**Quantity**	**Replacement / Cost**
Servers		
GESOAPP	2	$54,000
GESO2SRVR	2	$70,000
GEST-TEST	1	$17,000
GIACDATA	2	$27,000
GESO-DATA	1	$27,000
GIAC-MAIN	4	$58,000
Backbone Hubs	2	$13,000
Routers		
Cisco 7500	1	$41,000
GESO Routers	2	N/A
Mainframe Connection		
Corporate IBM 3174	1	N/A
Corporate Channel Extender	1	N/A
Rings		
User Rings	8	$0
IDNX	1	$0
3: Replacement costs included in backbone hub replacement.		
UPS (1 per 2 servers)	11	$11,000
Console Units	10	20,000
CD ROM Drives	14	$7,130
Modems	10	$1,870
TOTAL REPLACEMENT COST		**$337,000**

IMPACT CATEGORY: Destruction

JUSTIFICATION:

The replacement value represents the nominal cost of providing the same or better capability in the event of destruction. It is the cost of replacing the existing equipment with current technology, not in-kind.

Additionally, the time required to switch over to the alternate networks is approximately 5 business days. The cost of denial of service during the switch to the alternate networks is therefore minimal. Therefore, denial of service costs are calculated as follows:

135 Plant workers/computer x $100/day x 5 days = $67,500
40 GIAC corporate office workers/computer x $200/day x 5 days = $40,000
10 GIAC executive personnel/computer x $185/day x 5 days = $9,250

The total asset valuation is $3,530,738, which includes the cost of replacing installing, and testing the equipment ($3,413,988), and the cost of denial of service ($116,750).

Asset Value: $3,530,738

USER AREAS ASSET IDENTIFICATION AND VALUATION WORKSHEET

Description	Quantity[1]	Replacement Cost[2]	Maintenance Contract
Computers			
Pentium IV PCs	100 (Corp Office)	$200,000	Yes[1]
Pentium IV Laptops	10 (Corp Office)	$43,000	Yes[1]
Pentium IV PCs	120 (Plant)	$380,000	Yes[1]
Pentium IV Laptop	10 (Plant)	$67,000	Yes[1]
Printers	100	$50,000	No
Scanners	30	$10,000	No

(1) Replacement cost includes extended (3 year) OEM warranty.

TOTAL REPLACEMENT ESTIMATE $750,000

IMPACT CATEGORY: Destruction

JUSTIFICATION:

The replacement value represents the nominal cost of providing replacement end-user computing capability in the event of destruction through the procurement of equivalent replacement equipment within GIAC Enterprises, GIAC Enterprises and GESO standards, depending on the available technology at the time of the destructive loss. It is therefore calculated based on the cost of replacing the existing equipment with IT21 compliant equipment. The Risk Assessment Team used all resources instead of typical user areas due to the likelihood of loss similar to Homestead AFB, FL, due to the location of this activity in a Hurricane-prone area.

The average time to procure, install and test the replacement equipment is 6 months. During this time, the 185 users would be denied service. If total replacement were required, accelerated procurement procedures would be utilized to reduce denial of service time to 2 weeks at a cost of $233,500 computed as follows:

135 Plant workers/computer x $100/day x 10 days = $135,000
40 GIAC corporate office workers/computer x $200/day x 10 days = $80,000
10 GIAC executive personnel/computer x $185/day x 10 days = $18,500

The total asset valuation is $883,500, which includes the cost of replacing the equipment ($750,000) and the cost of denial of service ($233,500).

Asset Value: $983,500

DATA ASSET IDENTIFICATION AND VALUATION WORKSHEET

The seven GESO Corporate LAN file servers contain both Corporate and non-proprietary sensitive data. Data consist of official correspondence, internal memorandums, E-mail messages to local and remote site personnel, financial planning spreadsheets, procurement documents, and various other files in support of administrative functions.

Since data backups are not stored off-site, if total destruction of the primary data located on the production storage drives and the daily backup files located within the GESO were to occur, the result would be catastrophic to GESO. Site personnel were not able to supply the Risk Assessment team with any idea of the staff-hours required to reconstruct critical data files, if total destruction were to occur, partly due to the limited timeframe of the team' s analysis and limited understanding of available private backup files by the user-base. This impact category should be explored by site personnel to best quantify this asset. However, in order to supply GESO with a complete risk assessment, the risk assessment team selected the second worst-case impact category to provide a per-occurrence loss value for this asset.

Impact Category: Disclosure

Justification: An asset value of $100,000 is assigned for the disclosure of (worst case) Privacy Act data. To arrive at this figure, the IA R-US Risk Assessment Team used experience from performing Government Risk Assessments.

Asset Value: $100,000

SOFTWARE ASSET IDENTIFICATION AND VALUATION WORKSHEET

GIAC Enterprises Application Server Software:

USE	UNCLAS NETWORK	REPLACEMENT COSTS
NETWORK	Windows 2000	70,000
OPERATING SYSTEM		0
OFFICE AUTOMATION TOOLS	Lotus Smartsuite 5.0	3,000
	MS Office 2002	7,000
E-MAIL TOOLS	MS Exchange	10,000
GROUPWARE TOOLS	GIAC Database System 4.5	5,500
RECORD MESSAGE	MTF3.4/DPVS 4.0	0
LAN BASED APPLICATIONS	MDS 3.5	0
PRIMARY PRODUCTION SYSTEM	GIAC Production Database System Databases	0
INTERNET BROWSING	Internet Explorer 3.0	0
TIME MANAGEMENT	MS Exchange/Outlook 2002, Lotus Organizer, & Palm Desk	1,500
CORPORATE PROJECT MGMT	MS Project Manager	3,000
DIAL-IN	RAS Account	0
ANTI-VIRUS	Symantec CE & McAfee	0
	Total	$100,000

The servers maintained by the GESO contain network software pertinent to all sections of GIAC Enterprises. Some software is available through blanket Corporate or GIAC Enterprises contracts, such that they may be replaced without additional license costs.

Impact Category: Destruction

Justification: Backup software is stored in the GESO. Loss of primary production software would require short-term down-time and reloading from available backups. In the event of catastrophic loss of primary production software as well as backups, no off-site backups are currently available. This would require obtaining free copies through licensing agreements from GIAC Enterprises contracts and from the vendors.

Site personnel estimated that a maximum of 16 business hours would be required to acquire software from GIAC Enterprises or vendor sources and reestablish user access. Using a GESO worker at approximately $8.12 per hour would be required to reload critical files; Plant workers at $12.50 per hour, GIAC executive at $25 per hour, average user $23.13 per hour. This results in an asset value of $46,700 (135 x $100/day x 2 days) + (40 x $200/day x 2 days) + (10 x $185/day x 2 days) in addition to $100,000 replacement costs from vendors.

Asset Value: $146,700

PERSONNEL ASSET IDENTIFICATION AND VALUATION WORKSHEET

All GIAC Enterprises Systems Office jobs are considered essential to the proper administration and support to the GESO Corporate LAN. Maintaining current operational requirements finds the entire GESO understaffed.

Impact Category: Destruction

Justification: The cost of this asset is based on the time to implement replacement personnel should there be significant loss of permanent existing staff. Site personnel determined that in the unlikely event of loss of the technical staff while maintaining normal operations, that a combination of temporary assistance in the Plant from the GIAC Enterprises office personnel for off-hours support and management coordination. This short-term plan results in no additional cost to GESO. It is further estimated by the site management personnel that within a 2-week period, emergency delivery order modifications would be required to use outside contracted personnel. A total of 10 contractors, estimated average burdened cost of $50 per hour each, would be required for a period of approximately 80 business days until new permanent personnel could be brought in as replacements, and normal operating costs would resume. This results in a cost, outside of normal operating costs, of $320,000, (10 contractors x $50 per hour x 8 hours x 80 business days).

Asset Value: $320,000

FACILITY ASSET IDENTIFICATION AND VALUATION WORKSHEET

FACILITY NAME AND ADDRESS:

Key Largo Facility
Systems Office
GIAC Plant0
1775 GIAC Lane
Key Largo, FL 12345-6789

			DOLLAR VALUE	
Room:	Approximate Number of Square Feet		Replacement Cost Per Square Foot	
Help Desk/GESO	314	x	$150	
Server Room	196	x	$150	
Total:	500	x	$150	= $ 75,000

Other Upgrades included in the replacement cost identified above:

Air Conditioning
Raised Flooring
Power
Automatic Sprinkler Fire Suppression System

Impact Category: Destruction

Justification: The facility that houses the GESO Corporate LAN is located in the GESO, Building 5 portion of the GESO GIAC Plant, Key Largo Facility. The facility construction consists of reinforced concrete walls and wooden external doors. GESO Facilities personnel maintain information pertaining to replacement costs and provided the Risk Assessment Team the weighted average of $150 per square foot to substantiate the cost to replace the facility with the appropriate upgrades. Critical rooms for supporting the key equipment and operations of the Corporate LAN were included. The total value of this asset is $ 75,000.

Asset Value: $ 75,000

ADMINISTRATIVE ASSET IDENTIFICATION AND VALUATION WORKSHEET

Administrative assets include all documentation and supplies to support the operations and consumable products to maintain the GESO Corporate LAN.

DOCUMENTATION: Approximately 50 key vendor references are maintained on-site to support operation of and user support for the GESO Corporate LAN. An average replacement cost of $50 per manual is estimated for the vendor manuals. The total cost is $2,500 ($50 x 50 vendor manuals).

SUPPLIES Apart from miscellaneous tools, the GESO houses the following:

Equipment	Estimated Cost
1 Sniffer	$60,000
1 Fluke	$11,000
1 Fiber Optic Test Kit	$10,000
1 HP Open View	$30,000
20 Network Cards	$3,000
Various Cable Spools	$10,000
Consumable supplies	$125 (on hand)

Supplies Total: $124,125

Impact Category: Destruction

Justification: Asset value is based on average replacement costs of documentation and supplies. The total asset value is $126,625 ($2,500 + $124,125).

Asset Value: $126,625

Section 3

THREAT AND VULNERABILITY EVALUATION WORKSHEETS

The risk assessment team evaluated 22 threats while conducting this analysis. These included standard AIS threats, as well as threats that are site-unique to operations for the GESO Corporate LAN. All threats are assigned a threat value rating of severe (5), high (4), moderate (3), low (2), remote (1), or not applicable (0), against each of the asset categories. These ratings are subjectively based upon the likelihood of occurrence of the vulnerabilities identified with consideration to the severity of the potential impact from those vulnerabilities. The definitions of the value ratings are provided below:

Definitions:

REMOTE - The risk of a given threat to a specific asset is assessed as having no significant impact on that asset as a result of destruction, modification, disclosure of data, or denial of service. This assessment is made when the threat is considered: (a) extremely unlikely to occur based on the existing safeguards and history, and/or (b) to have relatively insignificant detrimental impact on that asset if it does occur.

LOW - The risk of a given threat to a specific asset is assessed as remotely possible or having little or no significant impact on that asset as a result of destruction, modification, disclosure of data, or denial of service impacts. This analysis is made when the threat is considered: (1) unlikely to occur based on adequate controlling safeguards and history, and/or (2) to have a little detrimental impact on that asset if it does occur. Attention should be considered.

MODERATE - The risk of a given threat to a specific asset is assessed as being possible or having a notable impact in causing harm to and/or reducing the effectiveness of that asset as a result of destruction, modification, disclosure of data, or denial of service to that asset. Concern is warranted.

HIGH - The risk of a given threat to a specific asset is assessed as having a potentially significant impact on that asset as a result of destruction, modification, disclosure of data, or denial of service. This analysis is made when the threat is considered to have a reasonable potential of occurrence and, upon such occurrence, will result in significant impact on that asset. Extreme concern is warranted.

SEVERE - This analysis rating is made when the threat is considered to have an extreme likelihood of occurrence and, will result in a catastrophic impact on that asset. Immediate action is warranted.

NOT APPLICABLE - The threat does not apply to the asset under evaluation.

The threat value rating assigned is based on documentation review, observations, interviews with GESO, GIAC Enterprises, and other pertinent personnel, historical data when available, and the experience and knowledge of the risk assessment team. In isolated cases, the assigned threat value rating is based on the potential resulting impact of a successful threat rather than on historical data, so the risk assessment will accurately reflect the criticality of the impact on the mission. The table below provides a summary of the ratings for each asset/threat pair based on identified vulnerabilities with regard to in-place safeguards. No "Severe" ratings were assigned.

THREAT \ ASSET	**H/W**	**Comm**	**S/W**	**Data**	**Pers**	**Facil**	**Admin**	**User**
Natural Disaster	2	2	2	2	2	2	2	2
Aircraft Crash	1	2	1	1	1	1	1	1
Sabotage/Vandalism/Disorder	3	3	3	**4**	2	2	1	3
Power Failure/Fluctuations	2	3	2	2	2	0	0	2
Inad. Environmental Controls	**4**	**4**	2	2	2	2	2	2
Water Damage	2	3	2	2	0	1	2	3
Fire	3	3	3	3	3	3	3	3
Improper Housekeeping	2	2	1	1	0	0	0	2
Theft	1	2	2	0	1	0	2	3
Unauthorized Physical Access	1	2	1	2	1	1	1	3
Unauthorized Network Access	0	0	2	2	0	0	0	1
Misuse Computer Resources	2	2	3	2	0	0	0	3
Communication Failure	1	3	1	2	0	0	0	1
Unauthorized Comm Alter	0	3	2	2	0	0	0	0
Interference	0	0	1	1	0	0	0	1
Hardware Failure	3	0	0	0	0	0	0	0
Unauthorized H/W Alteration	2	0	0	0	0	0	0	0
Software Failure	0	0	2	1	0	0	0	0
Unauthorized Software	0	0	2	2	0	0	0	2
Malicious Software Infestation	1	0	2	2	0	0	0	3
Unauthorized Action	1	1	2	3	0	0	0	3
Unauthorized Disclosure	0	0	1	3	0	0	0	0

The detailed identification and analysis of individual threats and their assigned threat values are provided on the Threat and Vulnerability Evaluation Worksheets.

Threat Name: NATURAL DISASTER

Description:

The GIAC Enterprises Systems Integration spaces may be destroyed in whole or in part by the occurrence of a natural disaster. This threat includes all types of natural occurrences (e.g., earthquake, hurricanes, rain storm) that may damage or otherwise impact one or more of the network assets.

Existing Safeguards:

- GIAC Enterprises is located on top of a high point, far from a flood zone. This location protects it adequately from flood and most tidal surges.

- No historical significant damage to GESO Corporate LAN assets, due to natural disaster, has been reported in the past 5 years.

- Essential personnel have been identified and a recall roster is available in the HelpDesk Standard Operating Procedures and in the GESO Recall and Social Roster available via GIAC Production Database System.

- An escape route plan for the Network Operations Center (GESO) is contained in the Emergency Action Plan (EAP), posted prominently in the Systems Office Message Support Section area.

- GIAC Plant exits and stairways are easily accessible and sufficient in width for adequate building evacuation.

- GIAC Plant is ruggedly constructed of reinforced concrete.

- There has been no record of volcanic activity on record in this vicinity.

- Emergency exits are clearly marked and emergency lighting is available in GIAC Plant and user areas.

Threat Name: NATURAL DISASTER (continued)

Vulnerabilities Noted:

- A Systems Office Corporate LAN Contingency plan has not been documented and tested.
- Data and software backups are not stored off-site.

Other Miscellaneous Concerns:

- Significant hurricane impact to the vicinity occurred in 1998 and concern over potential of future complications from hurricane activity is warranted. Therefore, significant hurricane activity historically occurs approximately once each decade.
- There exists an earthquake fault below Key Largo, FL. However, significant earthquakes have not occurred within the past two decades.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	3	Moderate
Communications	3	Moderate
Software	3	Moderate
Data	3	Moderate
Personnel	3	Moderate
Facility	3	Moderate
Administrative	2	Low
User Areas	3	Moderate

Threat Name: AIRCRAFT CRASH

Description:

Close proximity to an airport, runway, or aircraft practice area could result in an aircraft crash causing damage or other impact to the facility and/or assets.

Existing Safeguards:

- GIAC Plant exits and stairways are easily accessible and sufficient in width for adequate building evacuation.

- The Key Largo Facility is not in the direct flight pattern of aircraft from Key Largo Private Airport, or any other airport.

- An escape route is contained in the Emergency Action Plan, and maps are posted prominently in the Office and Plant spaces.

Vulnerabilities Noted:

- No significant vulnerabilities were noted.

Other Miscellaneous Concerns:

– Corporate helicopters occasionally land at the GIAC Enterprises GIAC Plant helicopter pad, located approximately 1.2 miles from Systems Office Building.

– Key Largo Facility is located on high ground approximately 5 miles from Key Largo private Airport and 30 miles from Naval Air Station – Marathon Key.

Assessment of Risk:

_ ASSET	RATING	IMPACT DESCRIPTION
Hardware	1	Remote
Communications	2	Low
Software	1	Remote
Data	1	Remote
Personnel	1	Remote
Facility	1	Remote
Administrative	1	Remote
User Areas	1	Remote

Threat Name: SABOTAGE/VANDALISM/CIVIL DISORDER/TERRORISM

Description:

Safeguards, vulnerabilities and estimated impacts to assets due to sabotage, vandalism, civil disorder, and terrorism are provided together due to their similarities. This category includes deliberate aggressive actions that may be instigated by foreign powers. Sabotage involves the premeditated destruction or modification of physical assets or data for either personal or political reasons. Vandalism is the random destruction or modification of system resources with no clearly defined objective. Civil disorder is the result of public unrest, which may lead to rioting and detrimental impact to network assets. Terrorism is the use of terror primarily as a means of coercion. Normally this involves the loss of lives and/or property, or the aggravated threat of loss of life and/or property.

Existing Safeguards:

- Primary Key Largo Facility entrances are guarded by armed security at all times or secured.

- The permanent GESO personnel challenge unfamiliar unescorted people.

- An updated System Security Plan providing security guidance is ready for signature.

- GESO Visitors without formal GIAC Enterprises Identification (ID) are signed in and escorted by GIAC Enterprises personnel.

- GIAC Enterprises security personnel monitor visitors through a closed circuit video system.

- The GESO Customer Service HelpDesk has documented Standard Operating Procedures (SOPs).

- Specific GESO Areas, including the GESO, are protected by an electronic slide-card / cypher lock system.

- Slide-cards and corresponding personal identification numbers (PIN) are assigned to personnel and controlled by the individual. The PIN is changed by the individual or when suspected compromise occurs.

- Background agency checks are performed for all GESO personnel and supporting contractors prior to allowing access to proprietary sensitive data.

Threat Name: SABOTAGE/VANDALISM/CIVIL DISORDER/TERRORISM (continued)

- AIS security awareness briefings are presented to personnel as part of the check-in process and additional security training is provided annually.
- Individual user IDs and passwords are assigned.
- MS Exchange forces password changes every 12 weeks.
- Users are trained not to share passwords.
- A Network Intrusion Detection System and Firewall together prohibit, audit, and alarm unauthorized access attempts from the Internet.
- Network Intrusion Detection System sensors exist in front of and behind the firewall, and behind the RAS dial-in server.
- MS Exchange software limits log-on attempts to three, requiring the workstation to be reinitialized before continuing.
- Logon attempts, even if unsuccessful, are recorded in the network audit log.
- Section 5.2.a. of GESO Policy 5239.2A dated 10 September 2003 requires that users enact the password capability of their Windows screen-saver.
- All network services (email, file, print, etc.) have audit logs.
- Minimum password length is appropriately set to 7 characters.
- The GESO Customer Service Help Desk SOP identifies specifications and telephone numbers to call in the case of emergency (e.g., bomb threat, fire, injury).
- GIAC Plant exits and stairways are easily accessible and sufficient in width for adequate building evacuation.
- GIAC Plant is ruggedly constructed of reinforced concrete.
- The Security Manager and PMO sponsor and distribute Marine Forces Pacific Bomb Threat Cards to personnel to assist in handling related telephone calls.

Threat Name: SABOTAGE/VANDALISM/CIVIL DISORDER/TERRORISM (continued)

- GIAC Enterprises Policy 1 (in accordance with Federal and State mandates), Equal Opportunity Program, designates the GIAC Corporate Equal Opportunity Officer and provides for equal opportunity for all employees without regard to race, color, religion, sex, age, or national origin. The primary method for submitting grievances is through the electronic mail system, directly toe the EEO or to the President of GIAC Enterprises.

- A network configuration diagram and documentation are available.

- Terminated personnel are required to check out with the GESO for account termination. As a fail-safe, any account not active for 12 weeks is terminated.

- Uninterrupted Power Supply (UPS) are in place for all critical network equipment.

- The building is ruggedly constructed of reinforced concrete.

- All network equipment is located within the GESO room in GIAC Plant.

- All network and end user computing equipment procurements are evaluated for security requirements and compatibility with existing equipment.

- Key Largo Facility avenues of approach are protected by a combination of natural and man made (fence) barriers.

- A perimeter fence is in place to blockade front entrances to GIAC Plant in the event of heightened security conditions.

- GESO entrance doors are 1.75 inch thick hollow metal doors secured in metal frame. Hinges are not removable from the exterior.

- An internal technical vulnerability scan was performed by Corporate in September 2002. Immediate action was taken on significant findings.

- Key Largo Facility Security Office maintains continuous armed roving patrols throughout Key Largo Facility.

Threat Name: SABOTAGE/VANDALISM/CIVIL DISORDER/TERRORISM (continued)

- The Security Manager and PMO sponsor and distribute Marine Forces Pacific Bomb Threat Cards to personnel to assist in handling related telephone calls. Additionally, Bomb Threat procedures are documented and are readily available in the HelpDesk Standard Operating Procedures.

- The GESO Security Office has proliferated framed posters throughout the GIAC Plant, continuously reminding all personnel to be information security conscious.

- Closed circuit television cameras monitor the loading dock, garage entrances, and the freight elevator.

- A physical Security/Crime Prevention survey was performed by the Key Largo Facility Security on the GESO on 5 October 2002.

- An authorized access list is maintained at the main entrance to the GESO.

- A "Secure Area" sign has been posted on the main entrance to the GESO.

Vulnerabilities Noted:

- GESO users do not all comply with the GESOO 5239.2A requirement to enact screen-saver passwords on desktop workstations.

- After-hours visitors to the GIAC Plant are not audited.

- Network administration software does not ensure that users are using secure passwords.

- The log-in/lock-out feature is reset by rebooting the terminal without notification to the network administration personnel.

- Banyan Audit trail for users accessing GESO Corporate LAN servers are maintained for only 24 hours.

- Audit trails are not reviewed daily for unusual or other security-related occurrences.

- Data and software backups are not stored off-site.

Threat Name: SABOTAGE/VANDALISM/CIVIL DISORDER/TERRORISM (continued)

- A GESO Corporate LAN Contingency plan has not been documented and tested.

- Internet accesses to the GESO Corporate LAN have not been formally tested using a normal battery of intrusion software tools.

- Contingency procedures for failure of critical network equipment not organic to Camp Somewhere Systems Office (GESO and Corporate) have not been documented or tested.

- No single authority exists to determine and grant dial-in access to the network.

- Effective procedures to revoke terminated employee access to the GESO Corporate LAN are not available.

- A complete inventory of network and end user computing equipment is not maintained.

- The wire closets which house the patch panels and ATM switches are not locked to preclude unauthorized access.

- Switches are not properly labeled to prevent accidental shutoff for computer and communications equipment.

Other Miscellaneous Concerns:

- None Noted.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	3	Moderate
Communications	3	Moderate
Software	3	Moderate
Data	4	High
Personnel	2	Low
Facility	2	Low
Administrative	1	Remote
User Areas	3	Moderate

Threat Name: POWER FAILURE/FLUCTUATIONS

Description:

A power failure or fluctuation may occur as the result of commercial power failure. This may cause either a denial of service to authorized users (failure) or a modification of resources due to partial destruction (fluctuation).

Existing Safeguards:

- Redundant uninterruptible power supply (UPS) capability is available and ready to operate for short and long-term use in support of primary GESO equipment.
- Functioning power filtering within the UPSs regulate power to primary GESO equipment.
- There exists a backup commercial power supply from a second sub-station, separate from the primary supply.
- HelpDesk Standard Operating Procedures provide guidance for emergency system shutdown and for electrical safety.
- The equipment is appropriately grounded.
- Data are backed up daily.
- Equipment in communications closets have short-term UPSs to regulate power and supply temporary power during brown-out conditions.
- This building has no history of significant electrical power problems.
- Short-term emergency lighting exists within the GESO.
- Windows provide adequate emergency lighting during normal working hours for network users.
- Master power switches and breakers are available at the GESO Corporate LAN GESO conference room and at the power distribution system.

Threat Name: POWER FAILURE/FLUCTUATIONS (continued)

Vulnerabilities Noted:

- A shunt-trip is not installed to cut power to the GESO in the event of flooding of the dry-pipe sprinkler system.

- Switches are not properly labeled to prevent accidental shutoff for computer and communications equipment.

Other Miscellaneous Concerns:

- End User equipment is not supported by the Generator UPS system.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	2	Low
Communications	3	Moderate
Software	2	Low
Data	2	Low
Personnel	2	Low
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	2	Low

Threat Name: **INADEQUATE ENVIRONMENTAL CONTROLS**

Description:

Air conditioning, heating, or humidity controls may malfunction, resulting in extreme temperatures causing damage to network assets.

Existing Safeguards:

- GIAC Enterprises GIAC Enterprises Facilities personnel maintain the GESO cooling equipment.

- The air conditioning system works properly and is maintained according to specifications.

- GESO personnel are required to document readings from thermometers in the GESO rooms in the log book per a predetermined schedule.

- HelpDesk Standard Operating Procedures provide guidance for air conditioning failure.

- A humidistat is available to regulate GESO humidity levels.

- Temperatures in user work spaces are appropriately maintained within vendor-recommended equipment parameters.

Vulnerabilities Noted:

- The GESO Corporate LAN GESO's server room currently exists in a warm environment. Facilities personnel report that any augmentation of existing equipment may cause ambient temperatures to exceed operating maximum levels for certain equipment due to saturation of the existing cooling capability.

- A backup air conditioning system is not available.

- Communications Closets are inadequately cooled.

Other Miscellaneous Concerns:

- Fire retardant material used in the construction of the GIAC Plant is asbestos.

Threat Name: INADEQUATE ENVIRONMENTAL CONTROLS (continued)

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	4	High
Communications	4	High
Software	2	Low
Data	2	Low
Personnel	2	Low
Facility	2	Low
Administrative	2	Low
User Areas	2	Low

Threat Name: WATER DAMAGE

Description:

Water from internal or external sources may damage the GESO Corporate LAN spaces and/or equipment.

Existing Safeguards:

- GESO personnel do not place liquid containers on or near the equipment.

- Plastic sheeting is available to cover the equipment.

Vulnerabilities Noted:

- A GESO Corporate LAN Contingency plan has not been documented and tested.

- Water detection devices are not installed under the GESO flooring

- Users frequently place liquid containers near desktop workstations.

Other Miscellaneous Concerns:

- Overhead pipes, including a dry-pipe sprinkler system, and other water sources are located in areas adjacent throughout of the GIAC Plant.

- Roof problems have occurred within the past year resulting in leakage into the GESO.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	2	Low
Communications	3	Moderate
Software	2	Low
Data	2	Low
Personnel	0	Not Applicable
Facility	1	Remote
Administrative	2	Low
User Areas	3	Moderate

Threat Name: FIRE

Description:

An accidental or intentional fire (or smoke) could damage the network equipment and/or the facility housing the network equipment.

Existing Safeguards:

- Heat sensors and smoke detectors are installed and functioning throughout GIAC Plant, including the GESO.

- Heat sensors and smoke detectors throughout the GIAC Plant automatically alert the Fire Alarm Division in Key Largo Facility Fire House by a Radio Alarm Kingfisher system.

- Key Largo Facility Fire Department response time is within 5 minutes.

- HelpDesk Standard Operating Procedures provide guidance for fire safety.

- Contractor personnel have scheduled the completion of a dry-pipe sprinkler to be installed throughout the GIAC Plant during the first quarter of 2004.

- An automatic CO^2 fire suppression system is available and active in the GESO. Two sensor zones must activate before the CO^2 will dump.

- Automatic pre-action dry-pipe sprinkler systems are available and active in the GESO and all user spaces. Two sensor zones must activate before the sprinkler system will flood.

- Emergency exits are marked clearly, and emergency lighting is available throughout GIAC Plant and user areas.

- An escape route plan is contained in the EAP, posted prominently in the Message Support Section area. Escape routes are also posted in distributed locations throughout the GIAC Plant.

- GIAC Plant exits and stairways are easily accessible and are sufficient in width for adequate building evacuation.

- The GIAC Plant is constructed using fire retardant material.

Threat Name: FIRE (continued)

- Personnel are regularly trained in fire drills and the use of fire extinguishers.

Vulnerabilities Noted:

- Data and software backups are not stored off-site.
- A GESO Corporate LAN Contingency plan has not been documented and tested.
- Fire extinguishers are not properly maintained and tested.
- Fire Warden duties are not being accomplished in accordance with GIAC Enterprises Policy 1212 of 24 July 2003.
- The GESO automatic CO2 delivery system is not properly maintained.

Other Miscellaneous Concerns:

- Fire retardant material used in the construction of the GIAC Plant is asbestos.
- Emergency procedures for handling fires are not prominently posted

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	3	Moderate
Communications	3	Moderate
Software	3	Moderate
Data	3	Moderate
Personnel	3	Moderate
Facility	3	Moderate
Administrative	3	Moderate
User Areas	3	Moderate

Threat Name: IMPROPER HOUSEKEEPING

Description:

Network assets may be impacted by improper housekeeping (e.g., cluttered areas creating potential fire hazards and prohibiting evacuation and dust causing malfunction of computer equipment).

Existing Safeguards:

- GIAC Enterprises personnel provide field-day cleaning to their spaces on as-required and scheduled basis.

- Personnel are trained to clean around computer equipment.

- Dust contributors are not permitted in equipment areas.

- Carpet areas are vacuumed each week or as required.

Vulnerabilities Noted:

- None

Other Miscellaneous Concerns:

- GESO Customer Service HelpDesk and server room spaces are extremely confined for the amount of equipment and personnel located within these spaces.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	2	Low
Communications	2	Low
Software	1	Remote
Data	1	Remote
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	2	Low

Threat Name: THEFT

Description:

Employees, contractor personnel, janitors, or outsiders may steal computer equipment or supplies. Note: Theft of data is considered under Unauthorized Disclosure.

Existing Safeguards:

– Primary Key Largo Facility entrances are guarded by armed Key Largo Facility Security at all times or secured.

- Armed GIAC Enterprises security guards check ID badges and allow unescorted Camp access only to those with valid GIAC Enterprises identification.

- Key Largo Facility Security Office maintains continuous armed roving patrols throughout Key Largo Facility.

- Closed circuit television cameras monitor the loading dock, garage entrances, and the freight elevator.

- Specific GESO Areas, including the GESO, are protected by an electronic slide card / cipher lock system.

- Slide cards and corresponding personal identification numbers (PIN) are assigned to personnel and controlled by the individual. The PIN is changed by the individual or when suspected compromise occurs.

- Responsible Employees are assigned accountability for information technology equipment within different GIAC Enterprises sections.

- The permanent GESO personnel challenge unfamiliar unescorted people.

- Administrative procedures are current and followed.

- A closed circuit television camera allows GESO personnel to monitor the facility entrances.

- Various levels of background checks are performed for all GESO personnel and supporting contractors to ensure a minimum level of trust.

Threat Name: THEFT (continued)

- A physical Security/Crime Prevention survey was performed by the Key Largo Facility Security on the facility on 5 December 2002.

- Authorized personnel are available within the GESO 24 hours each day.

Vulnerabilities Noted:

- GIAC Enterprises has experienced cases of theft of personal items, as well as PC devices, within the past year.

Other Miscellaneous Concerns:

- Any person issued a GIAC Enterprises badge is permitted complete, un-audited access to the Key Largo Facility.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	1	Remote
Communications	2	Low
Software	2	Low
Data	0	Not Applicable
Personnel	1	Remote
Facility	0	Not Applicable
Administrative	2	Low
User Areas	3	Moderate

Threat Name: UNAUTHORIZED PHYSICAL ACCESS

Description:

This threat pertains to the ability to intentionally or unintentionally enter into the facility, or other controlled perimeters surrounding the computer facility. Inattentiveness of personnel, inadequate procedures, or insufficient safeguards in place may permit access to the facility by unauthorized personnel.

Existing Safeguards:

- A physical Security/Crime Prevention survey was performed by the Key Largo Facility Security on the facility on 5 December 2002.

- A combination of a magnetic identification card and a personal identification number are issued and must be used by authorized personnel to gain unescorted access to the GESO.

- GIAC Enterprises security personnel monitor visitors through a closed circuit video system.

- GESO entrance doors are 1.75 inch thick hollow metal doors secured in metal frame. Hinges are not removable from the exterior.

- Primary Key Largo Facility entrances are guarded by armed Security at all times, or secured.

- The permanent GESO personnel challenge unfamiliar unescorted people.

- A combination door lock is installed. Combinations are controlled and changed approximately every 6 months or on suspected compromise as required by building security.

- Administrative procedures are followed and current.

- Sensitive data are protected physically by locked cabinets, secure building entrances, and door locks after normal working hours.

- Security awareness briefings are provided to personnel as part of the check-in process and additional security training is provided annually.

Threat Name: UNAUTHORIZED PHYSICAL ACCESS (continued)

- Closed circuit television cameras monitor the loading dock, garage entrances, and the freight elevator.

- Key Largo Facility Security Office maintains continuous armed roving patrols throughout Key Largo Facility.

- Walls surrounding and internal to the GESO extend from the hardened sub-floor to the hardened ceiling.

- GIAC Plant is ruggedly constructed of reinforced concrete.

- An authorized access list is maintained at the main entrance to the GESO.

- A "Secure Area" sign has been posted on the main entrance to the GESO.

- The GESO maintains staffing 24 hours each day.

Vulnerabilities Noted:

- Communications Closets are not locked.

Other Miscellaneous Concerns:

- Any person issued a GIAC Enterprises badge is permitted complete, unaudited access to the Key Largo Facility.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	1	Remote
Communications	2	Low
Software	1	Remote
Data	2	Low
Personnel	1	Remote
Facility	1	Remote
Administrative	1	Remote
User Areas	3	Moderate

Threat Name: UNAUTHORIZED NETWORK ACCESS

Description:

Unauthorized persons may gain access to the GESO Corporate LAN software and data through covert means (e.g., Spoofing addresses, Masquerading as authorized user, etc.)

Existing Safeguards:

– Key GESO network staff has been appropriately appointed in writing.

– Network passwords are suppressed on desktop workstation screens.

– Users are prohibited from sharing passwords.

- Individual user IDs and passwords are assigned.

- MS Exchange forces password changes every 12 weeks.

- Users are trained not to share passwords.

- MS Exchange software limits log-on attempts to three, requiring the workstation to be reinitialized before continuing.

- Logon attempts, even if unsuccessful, are recorded in the network audit log.

- Section 5.2.a. of GESO Policy 5239.2A dated 10 September 2003 requires that users enact the password capability of their Windows screen-saver.

- All network services (email, file, print, etc.) have audit logs.

- A Network Intrusion Detection System and Firewall together prohibit, audit, and alarm unauthorized access attempts from the Internet.

- Network Intrusion Detection System sensors exist in front of and behind the firewall, and behind the RAS dial-in server.

Threat Name: UNAUTHORIZED NETWORK ACCESS (continued)

- Marine Forces Pacific Order 5239.2A is available to address automated information system security issues.

- AIS security awareness briefings are presented to personnel as part of the check-in process and additional security training is provided annually.

- User privileges and system accesses are controlled.

- MS Exchange provides for network password encryption at the workstation prior to interface with the server.

- Technical support passwords for systems administrators must be an alpha-numeric and are changed weekly.

Vulnerabilities Noted:

- Audit trail is only maintained for one day on users accessing the GESO Corporate LAN servers.

- The ISSO has not been formally trained for this position.

- The system does not automatically log-off terminals after a set time.

- Effective procedures to revoke terminated employee access to the GESO Corporate LAN are not available.

- Audit logs are not reviewed regularly for unusual activity.

- Warning banner messages are not consistently displayed during network log-on as mandated by SECNAVINST 5239.3.

- The log-in/lock-out feature is reset by rebooting the terminal without notification to the network administration personnel.

Threat Name: UNAUTHORIZED NETWORK ACCESS (continued)
Other Miscellaneous Concerns:

- None

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	0	Not Applicable
Communications	0	Not Applicable
Software	2	Low
_Data	2	Low
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	1	Remote

Threat Name: **MISUSE OF COMPUTER RESOURCES**

Description:

Individuals may employ the resources of the computer system for unauthorized purposes, resulting in modification, destruction, or disclosure of data or a denial of service to users.

Existing Safeguards:

- The GESO Security Office has proliferated framed posters throughout the GIAC Plant, continuously reminding all personnel to be information security conscious.
- Personnel recall procedures are established and available in the various Standard Operating Procedures.
- An authorized access list is maintained at the main entrance to the GESO.
- The GIAC Production Database System application provides a system transaction log that is reviewed on a case-by-case basis to track problems.
- Marine Forces Pacific Order 5239.2A is available to address automated information system security issues.
- A visitor access list is maintained at the main entrance to the GESO.
- AIS Security awareness training is provided to personnel annually.
- Background checks are performed for all GESO personnel and supporting contractors.
- Administrative rights are only granted to technical support personnel assigned to the GESO.
- Technical support passwords for systems administrators must be an alpha-numeric and are changed weekly.
- The minimum password length is set to 7 characters.
- Key GESO network staff has been assigned in writing.
- LAN Auditor is available to identify introduction of unauthorized or illegal software.

Threat Name: MISUSE OF COMPUTER RESOURCES (continued)

- Procedures are in place to revoke terminated personnel access to the GESO Corporate LAN.

- A Network Intrusion Detection System and Firewall together prohibit, audit, and alarm unauthorized access attempts from the Internet.

- Network Intrusion Detection System sensors exist in front of and behind the firewall, and behind the RAS dial-in server.
- GESO Order 5239.2A requires that all personnel abide by copyright laws.

- A Network Security Plan has been prepared for immediate release.

Vulnerabilities Noted:

- The GIAC Production Database System transaction log is not reviewed regularly for unusual activity.

- The MS Exchange Audit Trail is not reviewed regularly for security concerns.

- The audit trail for users accessing GESO Corporate LAN servers is maintained for only 24 hours.

- Internet communication may be established without requiring logging into an account.

- The log-in/lock-out feature is reset by rebooting the terminal without notification to the network administration personnel.

- GESO personnel have not all been formally trained for their GIAC Enterprises positions.

Other Miscellaneous Concerns:

- Although authorized, network administration personnel may upgrade network and workstation software beyond the reasonable limitations of the existing hardware, resulting in slow-downs in user productivity due to the reduction of processing speed.

Threat Name: MISUSE OF COMPUTER RESOURCES (continued)

- Internet access provides the means of bogging down bandwidth from official uses (e.g., PointCast), and can lead to loss of user productivity.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	2	Low
Communications	2	Low
Software	3	Moderate
Data	2	Low
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	3	Moderate

Threat Name: COMMUNICATION FAILURE

Description:

Communication links may fail during operation by users or remote data feed. This results in denial of service to remote sites or users.

Existing Safeguards:

- Primary applications are loaded onto desktop personal computers such that users may work in stand-alone mode when network services are down.
- The data communications protocol used includes error checking.
- Redundancy is built in the GESO Corporate LAN cable plant.
- Data communication with remote GESO Service Centers is provided through a qualified telecommunications company.
- Contracts and accelerated procurement procedures are available for emergency replacement of equipment.
- An accurate network diagram is maintained.
- Some spare or redundant communication equipment is readily available.
- A bypass circuit and dial-in access exist to connect outside users to the network in the event the firewall server fails.

Vulnerabilities Noted:

- A GESO Corporate LAN Contingency plan has not been documented or tested.
- There exists a single point-of-failure within the communications equipment architecture.

Other Miscellaneous Concerns:

- None

Threat Name: COMMUNICATION FAILURE (continued)

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	1	Remote
Communications	3	Moderate
Software	1	Remote
Data	2	Low
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	1	Remote

Threat Name: **UNAUTHORIZED COMMUNICATION ALTERATION**

Description:

Communication alteration by unauthorized personnel may lead to denial of service to users or a breach of security by allowing unauthorized network access.

Existing Safeguards:

- All network equipment is located within the GESO room in GIAC Plant.
- AIS security awareness briefings are presented to personnel as part of the check-in process and additional security training is provided annually.
- Background agency checks are performed for all GESO personnel and supporting contractors.
- Visitors without valid GIAC Enterprises IDs are signed in and escorted by GESO points of contact.
- Hardware inventory is maintained by authorized personnel only.
- Key Largo Facility Security Office maintains continuous armed roving patrols throughout Key Largo Facility.
- Configuration management is a function of the GESO shop, and has been established to address hardware, communications, and software configuration issues.
- A communications equipment maintenance agreement is in place for certain equipment.
- Communications equipment is maintained by authorized personnel only.
- Some spare or redundant communication equipment is readily available.
- A network configuration diagram and documentation are available.
- At least two operations personnel or contractors are assigned during normal working hours.

Threat Name: UNAUTHORIZED COMMUNICATION ALTERATION (continued)

Vulnerabilities Noted:

- The wire closets which house the patch panels and ATM switches are not locked to preclude unauthorized access.

– A GESO Corporate LAN Contingency plan has not been documented and tested.

Other Miscellaneous Concerns:

- None

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	0	Not Applicable
Communications	3	Moderate
Software	2	Low
Data	2	Low
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	0	Not Applicable

Threat Name: INTERFERENCE

Description:

Interference from outside sources may disrupt the transmission, reception, or processing of data.

Existing Safeguards:

- This system has no history of radar interference.
- No magnetic or X-ray testing is performed near this system.
- Shielded Category 5 and fiber optic cabling are used for LAN communications.

Vulnerabilities Noted:

- No significant vulnerabilities were noted.

Other Miscellaneous Concerns:

- None

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	0	Not Applicable
Communications	0	Not Applicable
Software	1	Remote
Data	1	Remote
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	1	Remote

Threat Name: HARDWARE FAILURE

Description:

Malfunctions or failure of hardware may cause denial of service to system users.

Existing Safeguards:

- System operators are trained in system emergency shutdown procedures.

- Primary applications are loaded onto desktop personal computers such that users may work in stand-alone mode when network services are down.

- Some redundant or spare hardware is readily available. Hardware failures for each server are recorded in the maintenance logs.

- Hardware is maintained only by authorized personnel.

Vulnerabilities Noted:

- A Systems Office Corporate LAN Contingency plan has not been documented and tested.

Other Miscellaneous Concerns:

- Primary servers currently do not have backup systems. However, replacement servers are on order, and some original servers are planned for retention as backup servers.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	3	Moderate
Communications	0	Not Applicable
Software	0	Not Applicable
Data	0	Not Applicable
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	0	Not Applicable

Threat Name: UNAUTHORIZED HARDWARE ALTERATION

Description:

Personnel may alter the hardware configuration in an unauthorized manner, which may lead to inadequate configuration control, covert channels, or other situations that may detrimentally impact network assets.

Existing Safeguards:

- The building is secured after normal working hours.
- Permanent staff challenges unfamiliar persons in the GESO Corporate LAN GESO.
- Hardware is maintained by authorized personnel only.
- GESO provides configuration control management for GIAC Enterprises.
- A hardware inventory is maintained and periodically verified.
- An authorized access list is maintained at the main entrance to the GESO.
- A "Secure Area" sign has been posted on the main entrance to the GESO.
- Specific GESO Areas, including the GESO, are protected by an electronic slide card / cipher lock system.
- Slide cards and corresponding personal identification numbers (PIN) are assigned to personnel and controlled by the individual. The PIN is changed by the individual or when suspected compromise occurs.

Vulnerabilities Noted:

- No significant vulnerabilities were noted.

Other Miscellaneous Concerns:

- None

Threat Name: **UNAUTHORIZED HARDWARE ALTERATION (continued)**

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	2	Low
Communications	0	Not Applicable
Software	0	Not Applicable
Data	0	Not Applicable
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	0	Not Applicable

Threat Name: **SOFTWARE FAILURE**

Description:

Software (both standard release and locally developed) may malfunction causing disclosure, destruction, or modification of data or denial of service to users.

Existing Safeguards:

- System software is readily available in the GESO.
- GESO provides configuration control management for GIAC Enterprises Headquarters.
- Software utilized on this system is vendor-supplied or developed to GIAC Enterprises specifications.
- System software is readily available in locked cabinets in the GESO.
- Software releases are tested before implementation.
- Programming capability does not exist on the GESO Corporate LAN.
- Production version of all approved software updates are released to all sites at the same time.
- Only executable versions of approved application software is maintained on the GESO Corporate LAN.
- Primary applications are loaded onto desktop personal computers such that users may work in stand-alone mode when network services are down.

Vulnerabilities Noted:

- A GESO Corporate LAN Contingency plan has not been documented and tested.

Other Miscellaneous Concerns:

- Vendor-supplied software has been known to cause network instability or to contain viruses.

Threat Name: SOFTWARE FAILURE (continued)

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	0	Not Applicable
Communications	0	Not Applicable
Software	2	Low
Data	1	Remote
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	0	Not Applicable

Threat Name: UNAUTHORIZED SOFTWARE

Description:

Software may be modified intentionally to circumvent system security controls, manipulate data, redirect copies of data (covert channels), or cause denial of service.

Unauthorized software that may detrimentally impact GESO network operations due to incompatibilities may be introduced to the network by users or administrators, causing denial or service and possible modification to technical assets.

Existing Safeguards:

– System software changes are vendor-supplied and installed by the System Administrator.

– An inventory of the software is maintained.

– Procedures for reporting and correcting software problems are in place via the GESO Customer Service Help Desk.

– Procedures for control and use of software are in place.

– Only an executable version of approved application software is maintained on the GESO Corporate LAN.

– The GIAC Production Database System application provides a system transaction log that is reviewed on a case-by-case basis to track problems.

– MS Exchange provides an audit log that is used to track problems.

– New versions of approved software are reviewed thoroughly and tested in an independent environment on a server designated for that purpose.

– Production version of all approved software updates are released to all sites at the same time.

– Personnel are dissuaded from using personal software on GESO equipment.

– Programming capabilities do not exist on the GESO Corporate LAN.

Threat Name: UNAUTHORIZED SOFTWARE (continued)

- Symantec Corporate Edition AntiVirus is available to scan servers and desktop computers upon initialization and its "Shield" is available to monitor for infected media during work sessions.

- LAN Auditor activates upon login and reviews workstation software.

- LAN Auditor is available to identify introduction of unauthorized software.

- Programming capabilities do not exist on the GESO Corporate LAN.

- GESO provides configuration control management for GIAC Enterprises.

- GESO Policy 5239.2A requires that all personnel abide by copyright laws.

Vulnerabilities Noted:

- Internet communication may be established without requiring logging into an account.

- Dial-up modems do not have a first-level access security method.

Other Miscellaneous Concerns:

- Although authorized, network administration personnel may upgrade network and workstation software beyond the reasonable limitations of the existing hardware, resulting in slow-downs in user productivity due to the reduction of processing speed.

- Internet access provides the means of bogging down bandwidth from official uses (e.g., PointCast), and can lead to loss of user productivity.

Threat Name: UNAUTHORIZED SOFTWARE (continued)

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	0	Not Applicable
Communications	0	Not Applicable
Software	2	Low
_Data	2	Low
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	0	Not Applicable

Threat Name: MALICIOUS SOFTWARE INFESTATION

Description: Malicious software that may detrimentally impact GESO network operations, information, data, and storage media, or allow unauthorized access, may be introduced intentionally or unintentionally by system users.

Existing Safeguards:

- LAN Auditor activates upon login and reviews workstation software.
- Symantec Corporate Edition AntiVirus is available to scan servers and desktop computers upon initialization and its "Shield" is available to monitor for infected media during work sessions.
- System software changes are vendor-supplied and installed by the System Administrator.
- Procedures for reporting and correcting software problems are in place via the GESO Customer Service Help Desk.
- Procedures for control and use of software are in place.
- MS Exchange provides an audit log that is used to track problems.
- New versions of approved software are reviewed thoroughly and tested in an independent environment on a server designated for that purpose.
- Personnel are dissuaded from using personal software on Systems Office equipment.
- LAN Auditor is available to identify introduction of unauthorized software.
- System software is readily available in locked cabinets in the GESO.

Vulnerabilities Noted:

- Symantec Corporate Edition AntiVirus software does not immediately scan downloaded Internet files.
- Backup Tapes are currently rotated every 2 weeks.
- Vendor-supplied software has been known to cause network instability or to contain viruses.

Threat Name: MALICIOUS SOFTWARE INFESTATION (continued)

Other Miscellaneous Concerns:

- None

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	1	Remote
Communications	0	Not Applicable
Software	2	Low
Data	2	Low
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	3	Moderate

Threat Name: **UNAUTHORIZED ACTION**

Description:

Inadvertent or intentional actions, malicious or otherwise, may result in GESO Corporate LAN data being modified or destroyed, causing denial of service. Data may be inadvertently or intentionally disclosed.

Existing Safeguards:

– Users are trained on use of LAN assets.

– Users are prohibited from sharing passwords.

– A Banyan Network system transaction log is available.

– Users are supervised closely.

– The GIAC Enterprises GESO Services User Guide, dated 1 August 2003 has been promulgated to provide procedures for service assistance.

– GIAC Enterprises Policy 1 (in accordance with Federal and State mandates), Equal Opportunity Program, designates the GIAC Corporate Equal Opportunity Officer and provides for equal opportunity for all employees without regard to race, color, religion, sex, age, or national origin. The primary method for submitting grievances is through the electronic mail system, directly toe the EEO or to the President of GIAC Enterprises.

– AIS security awareness training is provided to personnel annually IAW Public Law 100-235.

– Symantec Corporate Edition or McAfee AntiVirus software, available through existing corporate contracts, provides the ability to automatically scan files downloaded from the Internet.

- AIS security awareness training is presented to personnel annually and upon initial check-in.

– LAN Auditor is available to identify introduction of unauthorized software.

Threat Name: UNAUTHORIZED ACTION (continued)

Vulnerabilities Noted:

– Symantec Corporate Edition AntiVirus does not automatically scan downloaded Internet files.

– Standard Security Operating Procedures have not been developed.

- Users frequently place liquid containers near desktop workstations.

Other Miscellaneous Concerns:

- None

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	1	Remote
Communications	1	Remote
Software	2	Low
Data	3	Moderate
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	3	Moderate

Threat Name: **UNAUTHORIZED DISCLOSURE**

Description:

Unauthorized persons may gain access to proprietary sensitive information.

Existing Safeguards:

- Sensitive hard copy and magnetic media are disposed of properly.
- Background agency checks are performed for all GESO personnel and supporting contractors.
- Security awareness briefings are provided annually to all employees.
- Shredders are maintained in the various GESO sections for destruction so proprietary sensitive paper material.
- LAN Auditor is available to identify introduction of unauthorized software.
- Key Largo Facility Security Office maintains continuous armed roving patrols throughout Key Largo Facility.
- Terminated personnel are required to check out with the GESO for account termination. As a fail-safe, any account not active for 12 weeks is terminated.
- AIS Security awareness videos are presented to personnel annually.
- An authorized access list is maintained at the main entrance to the GESO.
- A "Secure Area" sign has been posted on the main entrance to the GESO.
- A Network Intrusion Detection System and Firewall together prohibit, audit, and alarm unauthorized access attempts from the Internet.
- Network Intrusion Detection System sensors exist in front of and behind the firewall, and behind the RAS dial-in server.
- The GESO Security Office has proliferated framed posters throughout the GIAC Plant, continuously reminding all personnel to be information security conscious.

Threat Name: UNAUTHORIZED DISCLOSURE (continued)

Vulnerabilities Noted:

- The system does not log off terminals after a set time.
- The GESO Web page contains proprietary sensitive data, including diagrams of the GESO floor plan.
- The GIAC Production Database System transaction log is not reviewed regularly for unusual activity.
- The MS Exchange Audit Trail is not reviewed regularly for security concerns.
- The audit trail for users accessing GESO Corporate LAN servers is maintained for only 24 hours.
- No identification or verification is required to have an account terminated.
- Dial-up modems do not have a first-level access security method.
- Internet communication may be established without requiring logging into an account.
- The log-in/lock-out feature is reset by rebooting the terminal without notification to the network administration personnel.

Other Miscellaneous Concerns:

- None.

Assessment of Risk:

ASSET	RATING	IMPACT DESCRIPTION
Hardware	0	Not Applicable
Communications	0	Not Applicable
Software	1	Remote
Data	3	Moderate
Personnel	0	Not Applicable
Facility	0	Not Applicable
Administrative	0	Not Applicable
User Areas	0	Not Applicable

ADDITIONAL RECOMMENDED COUNTERMEASURES

This section provides a list of additional recommended countermeasures. All proposed countermeasures are evaluated to determine their effectiveness in reducing the potential impact of existing vulnerabilities. Each proposed additional countermeasure is evaluated on a stand-alone basis to allow the GESO Director to implement any combination of the proposed countermeasures individually. Because this risk assessment is not quantitative in nature, return on investment (ROI) calculations are not performed. Please note that identified countermeasure costs are estimated, and may vary upon implementation.

ADDITIONAL COUNTERMEASURES EVALUATION WORKSHEET

1. **COUNTERMEASURE NAME:** Document Contingency Plan and Procedures

3. **IMPACTS:** Confidentiality, Integrity, Availability

2. **DESCRIPTION**

This countermeasure requires that the mission-critical GESO Corporate LAN have a system-specific contingency plan and procedures to implement the plan. The plan and procedures should detail emergency response and appropriate activities required for a contingent situation and should provide a suitable return to normal automated operations. The attached outline is offered as a suggested format for these procedures and examples of information that may be included. This countermeasure is estimated to require 100 hours each for the GESO Tech, a network administrator, and administrative support to research, develop and document the procedures.

3. **VULNERABILITY(IES) AFFECTED BY THIS COUNTERMEASURE:**

A GESO Corporate LAN Contingency plan has not been documented and tested.

Data and software backups are not stored off-site.

4. **IMPACTS PROTECTED:** Availability

5. **ESTIMATED ANNUAL COST:**

1 GESO tech x $25.21/hour x 100 hours	= $2,521
1 SA x $14.87/hour x 100 hours	= 1,487
3 contractors x $80/hour x 100 hours	= 24,000
TOTAL:	**$ 28,008**

EXAMPLE CONTINGENCY PLAN PROCEDURES OUTLINE

I. Emergency Response

A. Definition and Types (e.g., fire, hardware failure, security incident)

B. Responsibilities/Actions

1. GESO Personnel

a. During Working Hours
b. After Working Hours
c. Personnel to Contact
d. Recall List

2. System Administrator

a. Emergency Investigation
b. Personnel to Contact
c. Emergency Declaration
d. Determine Contingency Action

II. Contingency Action

A. Short-term Downtime

1. System Administrator Responsibilities
(e.g., call vendor, notify users,
determine corrective action)

2. Operations/GESO Director Responsibilities
(e.g., notify management, report printing,
troubleshoot)

3. User Requirements
(e.g., manual procedures, if required)

B. Long-term Downtime

1. System Administrator Responsibilities
(e.g., equipment replacement, impact analysis, status reporting)

2. Operations/GESO Director Responsibilities
(e.g., coordinate impact analysis, evaluate critical applications)

3. User Requirements
(e.g., detailed manual procedures for collecting raw data)

III. Recovery Actions

A. Responsibilities

1. System Administrator
(e.g., method of ensuring integrity system, inform users, system reload)

2. Network Operations Manager
(e.g., coordinate backup method implementation, execute system testing, schedule for return to normal operations)

3. Users
(e.g., verify data files, input raw data)

ADDITIONAL COUNTERMEASURES EVALUATION WORKSHEET

1. **COUNTERMEASURE NAME**

Review Audit Trail (Mandatory)

2. **DESCRIPTION**

This countermeasure requires the activation of all pertinent audit control features and the daily review of the audit trails during each normal business day.

3. **VULNERABILITIES AFFECTED BY THIS COUNTERMEASURE:**

- Audit trail logs are not reviewed regularly for unusual occurrences.

4. **IMPACTS PROTECTED:** Confidentiality, Integrity, Availability

6. **TOTAL ALE SAVINGS**

$8,433

8:1

COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME**

Provide formal security training to GESO Staff

2. **DESCRIPTION**

This countermeasure requires that Information Systems professionals be provided with formal network security schools to better equip them for security issues. Formal schooling will give these professionals the tools that are necessary to work security decisions into their current functions. Additionally, formal training will provide these professionals with current GIAC Enterprises requirements and the most cost effective means to implement these requirements.

3. **VULNERABILITIES COUNTERACTED**

GESO personnel have not all been formally trained for their positions.

4. **IMPACTS PROTECTED:** Confidentiality, Integrity, Availability

5. **ANNUAL COST**

It is estimated that to send 10 GESO personnel to SANS Institute training each year will cost approximately $4,000 per training session, or $40,000. This cost can be reduced to approximately $25,000 if course work is done online.

COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME**

Modify Automatic Enable of Lock-out Feature

2. **DESCRIPTION**

Users who fail three consecutive log-on attempts are currently automatically locked from further log-on attempts for 30 minutes. This countermeasure requires that the account remain Corporatebled until the System Administrator or CSSO enable the account manually. This provides accounting of all valid and invalid unsuccessful log-on attempts.

3. **VULNERABILITIES COUNTERACTED**

The log-in/lock-out feature is reset by rebooting the terminal without notification to the network administration personnel.

4. **IMPACTS PROTECTED:** Confidentiality, Integrity, Availability

5. **ANNUAL COST**

This countermeasure will require a global network modification. The System Administrator ($39.84 per hour) will require an estimated 5 hours to research and adjust the lock-out feature. This results in a cost of $199.20 ($39.84 x 5 hours). This cost, amortized over 5 years, results in an annual cost of $39.84 ($199.20 divided by 4).

ADDITIONAL COUNTERMEASURES EVALUATION WORKSHEET

1. **COUNTERMEASURE NAME**

Install Water Detection Devices

2. **DESCRIPTION**

Purchase and install water detection devices under the computer cabinets of the GESO Corporate LAN GESO. These detectors should be alarmed and/or connected to the electric power for the GESO Corporate LAN servers to avoid short circuits. Purchase and installation costs are estimated to be $500. This onetime cost is amortized over 5 years to result in an annual cost of $100 ($500 divided by 5).

3. **VULNERABILITIES COUNTERACTED**

Water detection devices are not installed under the GESO flooring

4. **IMPACTS PROTECTED:** Availability

5. **ANNUAL COST**

Purchase and installation costs are estimated to be $500. This onetime cost is amortized over 5 years to result in an annual cost of $100 ($500 divided by 5).

ADDITIONAL COUNTERMEASURES EVALUATION WORKSHEET

1. **COUNTERMEASURE NAME**

Implement Automatic Time-out Feature

2. **DESCRIPTION**

This countermeasure requires the enforcement of a workstation password time-out feature. GESO policy 5239.2A requires the implementation key contractor ($50 per hour) to revise user account security settings to enable and lock inactive or idle user workstations after 15 minutes of inactivity.

3. **VULNERABILITIES COUNTERACTED**

4. **IMPACTS PROTECTED:** Confidentiality, Integrity

5. **ANNUAL COST**

The contractor System Administrator will require approximately 8 hours to research the feasibility of this countermeasure and implement the requirement. The cost is estimated to be $400 ($50 per hour x 8 hours). This cost amortized over 5 years results in an annual cost of $80 ($400 divided by 5).

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME**: Establish Off-site Storage for Backups

2. **DESCRIPTION**

This countermeasure requires the establishment of a backup agreement with a remote location and the procurement of a high-speed conditioned line for transmission of corporate data for backup purposes. Additionally, the System Administrator will require approximately 4 hours per week to run a backup of software and data and to store the backups in the off-site location.

3. **VULNERABILITIES COUNTERACTED:**

- Data and software backups are not stored off-site.

- Backup Tapes are currently rotated every 2 weeks.

4. **IMPACTS PROTECTED**: Integrity, Availability

5. **ANNUAL COST**

$8,350

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. COUNTERMEASURE NAME

Dial-in Access Security.

2. DESCRIPTION

Currently, dial-in access is provided by the GESO HelpDesk to anyone requesting it. Dial-in access bypasses the firewall and IDS security software to anyone with a network account. A single responsible GIAC corporate office workers should be assigned the authority to grant or deny dial-in access to restrict this type of un-audited access only to those with the definite need for this service. Additionally, another level of security (e.g., call back, modem software password, strong user authentication, etc.) should be active at the point of remote entry to the network. This will provide an additional level of security prior to attempting network access.

3. VULNERABILITIES COUNTERACTED

Network dial-up modems do not have a first level access security method.
Dial-in access exists which bypasses the firewall and IDS software.
A single authority to grant dial-in access to the network does not exist.

4. IMPACTS PROTECTED: Confidentiality, Integrity

5. ESTIMATED COST

This countermeasure can be approached in multiple ways, wherein the more secure the methods of security, the more costly the countermeasure becomes. Implementation of smart-card or other token, such as using SecureID, provides strong authentication, but does not necessarily encrypt the session. The least costly implementation is provided, although the most stringent is recommended.

This countermeasure requires the research and forwarding of public keys for proper dial-in authentication and session encryption using existing Virtual Private Network capabilities. It is estimated to require approximately 20 hours from the CSSO to research and provide guidance and 20 hours from the System Administrator to implement the proper procedures for remote users to authenticate and conduct and encrypted session. The estimated time required for traveling personnel to configure laptop computers based on the guidance from the CSSO are considered negligible. Due to changing technologies, it is estimated that this process will change annually, and therefore the costs are recurring.

1 NSM (03) x $25.21/hour x 20 hours	= $504.20
1 SA (E6) x $14.87/hour x 20 hours	= 297.40
TOTAL:	**$ 791.60**

Install a security method for dial-in modem access: $200/copy X 10 copies = $2,000

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. COUNTERMEASURE NAME

Install Internet-capable Anti-Virus Software

2. DESCRIPTION

Currently, GESO users may access and download Internet software and data. By scanning downloads at the point of entry to the gateway by implementing Internet-capable scanning software on the Firewall Bastion Host. The network is protected if viruses are present and the user fails to download the files to a floppy and scan the files at the desktop. Symantec Corporate Edition and McAfee antivirus software provide this feature. Additionally, it is possible for stealth or polymorphic viruses to evade Anti-virus software and corrupt backup files; therefore the package chosen should be a different one than that which is normally used for scanning the network.

3. VULNERABILITIES COUNTERACTED

- Symantec Corporate Edition AntiVirus software does not immediately scan downloaded Internet files.

- Backup Tapes are currently rotated every 2 weeks.

4. **IMPACTS PROTECTED:** Confidentiality, Integrity

5. ESTIMATED COST

GIAC Enterprises has already procured both McAfee and Symantec Corporate Edition complete licenses of Anti-Virus software. The cost is limited to the time required for a Network Security Manager to implement and regularly update this software and signature files.

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. COUNTERMEASURE NAME

Procure and maintain backup network servers.

2. DESCRIPTION

Currently, there are several single points of failure within the GESO Corporate (Corporate) LAN. Backup servers will reduce the amount of down time associated with network hardware failure.

GESO has servers on order to replace existing servers. When the new servers are installed, the existing servers may be used as backups.

3. VULNERABILITIES COUNTERACTED

- There are no spare servers to serve as backup in the event the primary equipment should fail or need repair.
- GESO operates and relies on mission critical equipment owned by other organizations.

4. IMPACTS PROTECTED: Availability

5. ESTIMATED COST

Servers cost approximately $35,000 each. However, there is currently no additional cost for this because new servers are currently budgeted for procurement. Existing servers may be shelved to provide for the backup requirement of this countermeasure.

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME**

Maintain an accurate equipment inventory for network and end user computing and communications equipment.

2. **DESCRIPTION**

An accurate inventory of all GESO Corporate LAN equipment is essential for property record keeping and replacement of the equipment in the event of equipment failure. Additionally, an accurate inventory will provide a ready reference to responsible GIAC corporate office workers to ensure all equipment is recorded in the event of theft, loss, damage, etc.

3. **VULNERABILITIES COUNTERACTED**

An accurate inventory of network equipment is not maintained and readily available for reference in the event any or all network equipment must be replaced.

4. **IMPACTS PROTECTED:** Availability

5. **ESTIMATED COST**

Initial: 1 GESO employee x 10 days = $65.82/day X 10 days = $658.20

Annually: 1 GESO Employee x 10 days = $65.82/day X 10 days = $658.20

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. COUNTERMEASURE NAME

Restrict Internet access to official uses only

2. DESCRIPTION

Internet access provides an additional tool for information gathering. However, it may be abused/misused for other than official purposes. The current GIAC Enterprises policy restricts Internet access to official uses only. This provides policy guidance, but does not take proactive measures to limit access to unauthorized sites or preclude downloading of unauthorized software or data. Software implemented on the firewall is available that would make certain sites off-limits, restrict access to certain site types, or preclude downloading unauthorized software.

GESO currently has the capability to implement this countermeasure with existing software; however, it has not been implemented because it reduces performance (transmission speed) below acceptable levels.

3. VULNERABILITIES COUNTERACTED

The firewall does not place any restrictions on Internet access for network users. Currently, network users can access the Internet and download software and data for use within the network.

4. **IMPACTS PROTECTED:** Confidentiality, Integrity

5. ESTIMATED COST

GESO already has the capability to implement this countermeasure. Therefore, the cost of implementation is $0.

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME:** Physically secure the communications closets.

2. **DESCRIPTION**

The wire closets contain patch panels, asynchronous (ATM) switches, and uninterrupted power supplies (UPS). This equipment connects the users to the network. Restricting access to these areas to qualified technicians only can help to reduce unauthorized access and potential harm (unintentional human error and sabotage).

3. **VULNERABILITIES COUNTERACTED**

The wire closets are not locked to prevent unauthorized access.

Any person issued a GIAC Enterprises badge is permitted complete, unaudited access to all unrestricted areas within the GESO GIAC Plant.

4. **IMPACTS PROTECTED:** Availability

5. **ESTIMATED COST**

The patch panel doors already have locks installed; therefore, the cost of implementation is $0.

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME:** Install shunt-trip in the GESO

2. **DESCRIPTION**

This countermeasure requires that a shunt-trip be installed to cut power in the event of
inappropriate or excessive activation of the flooding of the preaction dry-pipe sprinkler system in the GESO. Currently, if the dry-pipe system is activated, it cannot be manually disabled. This countermeasure will cut electric power to the system, as necessary. It will prevent the equipment from shorting out and the personnel from potential electrocution.

3. **VULNERABILITIES COUNTERACTED:**

A shunt-trip is not installed to cut power to the GESO in the event of flooding of the dry-pipe sprinkler system.

4. **IMPACTS PROTECTED:** Availability

5. **ESTIMATED COST**

One time procurement - $4,000

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME**

Implement Fire Prevention Awareness Program

2. **DESCRIPTION**

This countermeasure requires that all GIAC Enterprises Fire Wardens be identified, trained, and held accountable for their responsibilities as fire wardens. This first step is critical to an effective fire awareness program. All hands should be exposed to their responsibilities in the event of fire. Currently, there is no identifiable training program. Fire drills are conducted on weekends and Marines indicate that they have not been advised of fire prevention responsibilities. A better working relationship between the Federal Fire Inspector, Key Largo Fire Protection Specialist, GIAC Enterprises Facilities, Fire Wardens, and the various sections of Key Largo Facility is essential. An annual Fire Awareness Day should be considered for all hands.

3. **VULNERABILITIES COUNTERACTED**

Personnel are inadequately trained in fire drills due to scheduling of annual drill requirement over weekends.

Coordination of Fire Warden appointments are not performed with the GIAC Enterprises Fire Protection Specialist.

4. **IMPACTS PROTECTED:** Availability

5**.** **ANNUAL COST:**

None

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME:**

Implement Effective Fire Prevention Inspection Program

2. **DESCRIPTION**

This countermeasure requires that all Key Largo Facility fire prevention equipment be inspected and updated on a regular basis. Currently, many fire extinguishers are out of date and remain untested. According to the GIAC Enterprises Fire Prevention Specialist, some extinguishers may be inoperative. The entire CO2 fire suppression system in the GESO has not met any of the required inspection criteria.

3. **VULNERABILITIES COUNTERACTED**

Coordination of Fire Warden appointments is not performed with the GIAC Enterprises Fire protection Specialist.

The GESO automatic CO2 delivery system is not properly maintained.

The Fire Inspector has at least 8 unresolved deficiencies specific to the GESO. Additionally, he estimates that there are over 100 unresolved action items related to Key Largo Facility.

4. **IMPACTS PROTECTED:** Availability

5. **ANNUAL COST**

Negligible

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME:**

Inspect and correct overheating in communications closets

2. **DESCRIPTION:**

This countermeasure requires that all communications closets be inspected by appropriate personnel to ensure that overheating in the closet does not occur. This will require that either heat emanating devices or equipment be relocated or alternative cooling means be employed.

3. **VULNERABILITIES COUNTERACTED**

Communications closets are inadequately cooled.

4. **IMPACTS PROTECTED:** Availability

5. **ANNUAL COST**

TBD

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME**

Label all emergency switching devices

2. **DESCRIPTION**

This countermeasure requires that all emergency switches be clearly labeled. In an emergency situation this switches must be clearly labeled to allow for immediate action while avoiding confusion. This countermeasure requires the coordination with Facilities personnel to identify poorly labeled switches in the GESO.

3. **VULNERABILITIES COUNTERACTED**

Switches are not properly labeled to prevent accidental shutoff for computer and communications equipment.

4. **IMPACTS PROTECTED:** Availability

5. **ANNUAL COST**

Negligible

ADDITIONAL COUNTERMEASURES DESCRIPTION WORKSHEET

1. **COUNTERMEASURE NAME**

Implement Manual Visitor Auditing

2. **DESCRIPTION**

This countermeasure requires that the GIAC Enterprises Security operating procedures be updated or enforced to preclude visitors from entry into GESO spaces outside of normal working hours without providing entry and exit accountability information into an official log. Currently, after entering the base, there is no audit trail of visitors to GIAC Enterprises user spaces. After hours visitors can enter the GIAC Plant without signing in or signing out.

3. **VULNERABILITIES COUNTERACTED**

After hours visitors to the Headquarters are not audited.

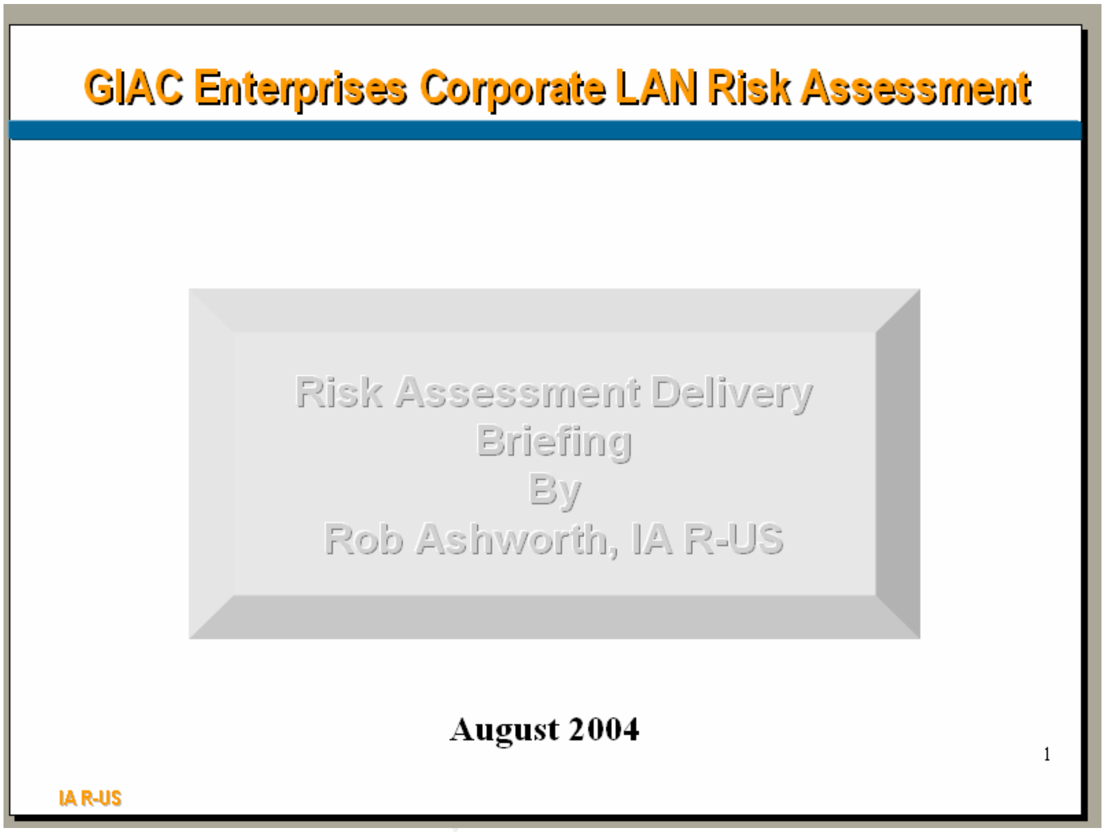
GIAC Enterprises has experienced cases of theft of personal items, as well as PC devices, within the past year.

4. **IMPACTS PROTECTED:** Confidentiality, Integrity, Availability

5. **ANNUAL COST**

Negligible

Deliverable Presentation: Part 4 – Section B:



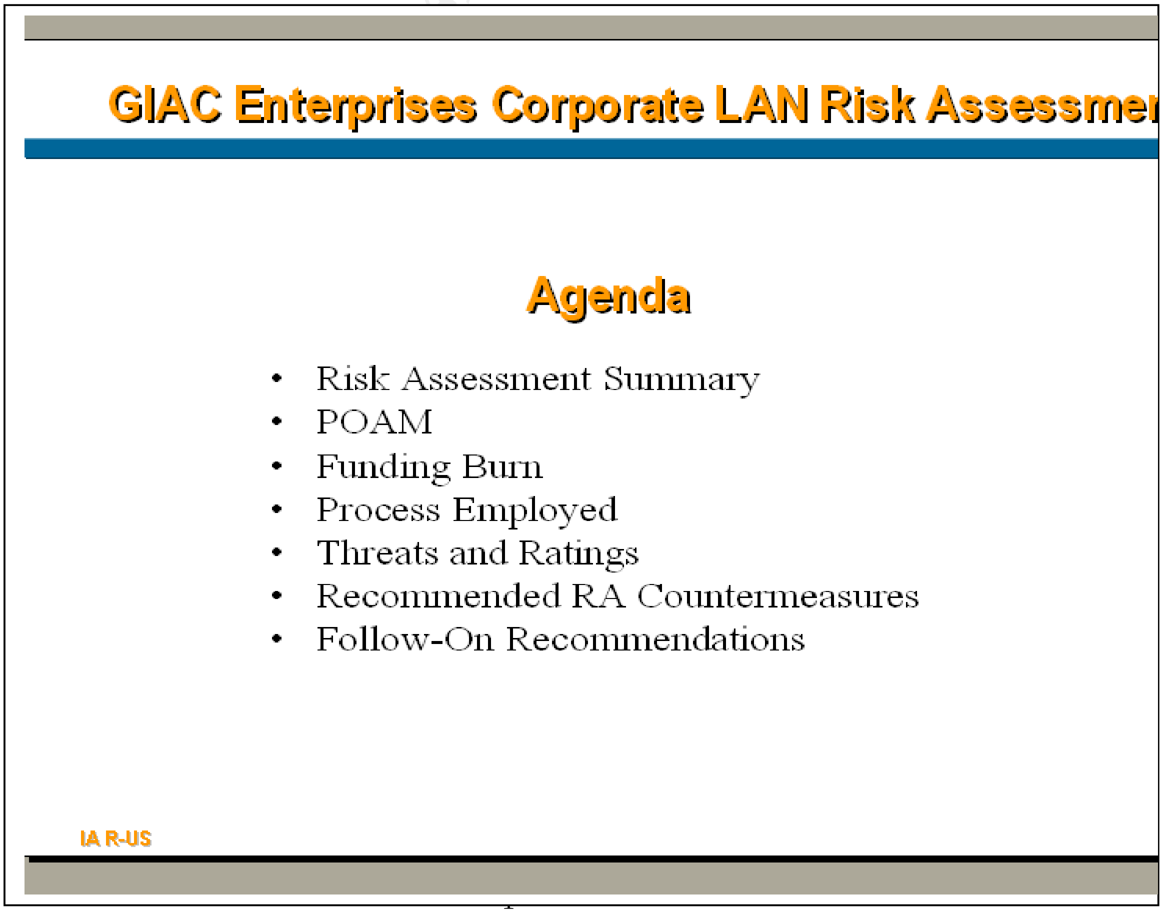
GIAC Enterprises Corporate LAN Risk Assessment

Risk Assessment Delivery Briefing
By
Rob Ashworth, IA R-US

August 2004

1

IA R-US

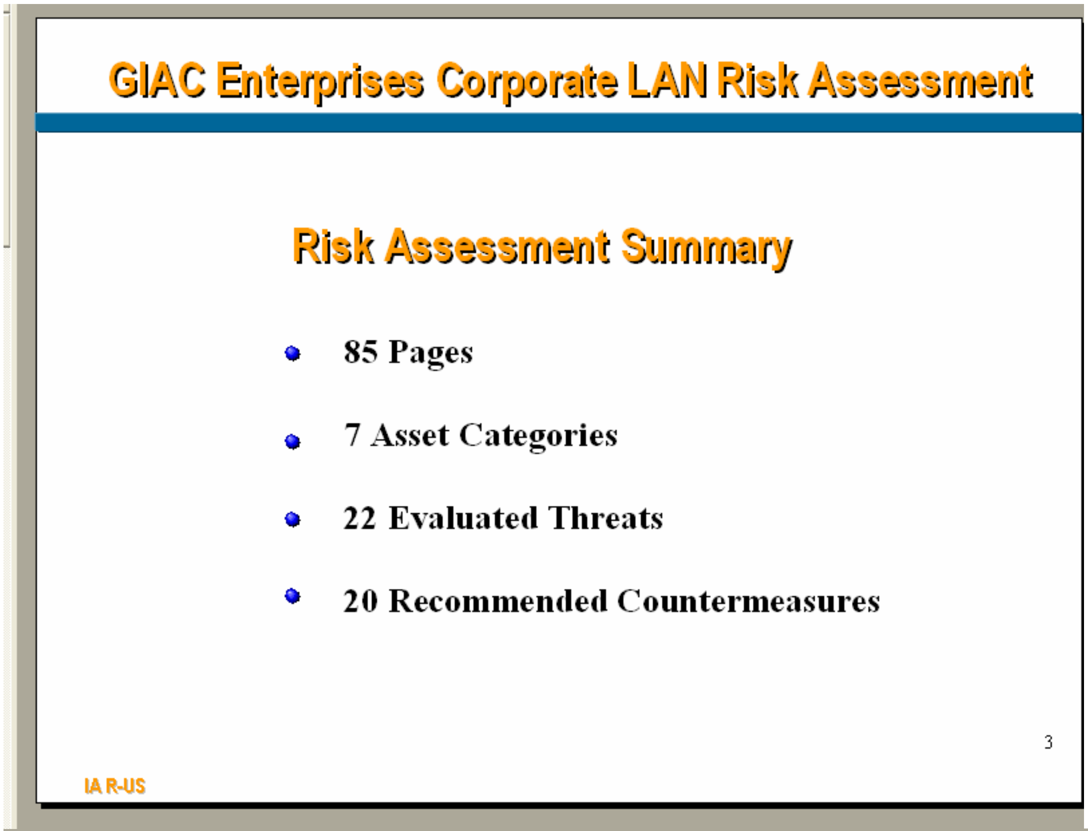


GIAC Enterprises Corporate LAN Risk Assessmen

Agenda

- Risk Assessment Summary
- POAM
- Funding Burn
- Process Employed
- Threats and Ratings
- Recommended RA Countermeasures
- Follow-On Recommendations

IA R-US



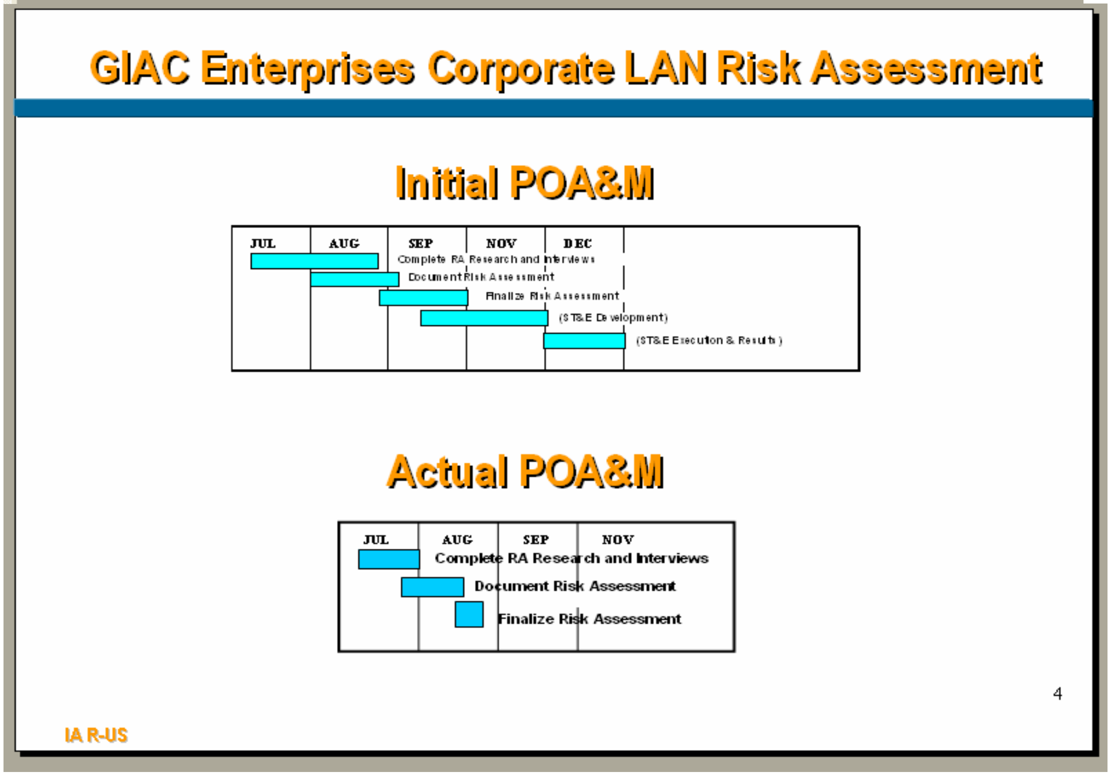
GIAC Enterprises Corporate LAN Risk Assessment

Risk Assessment Summary

- 85 Pages
- 7 Asset Categories
- 22 Evaluated Threats
- 20 Recommended Countermeasures

3

IA R-US



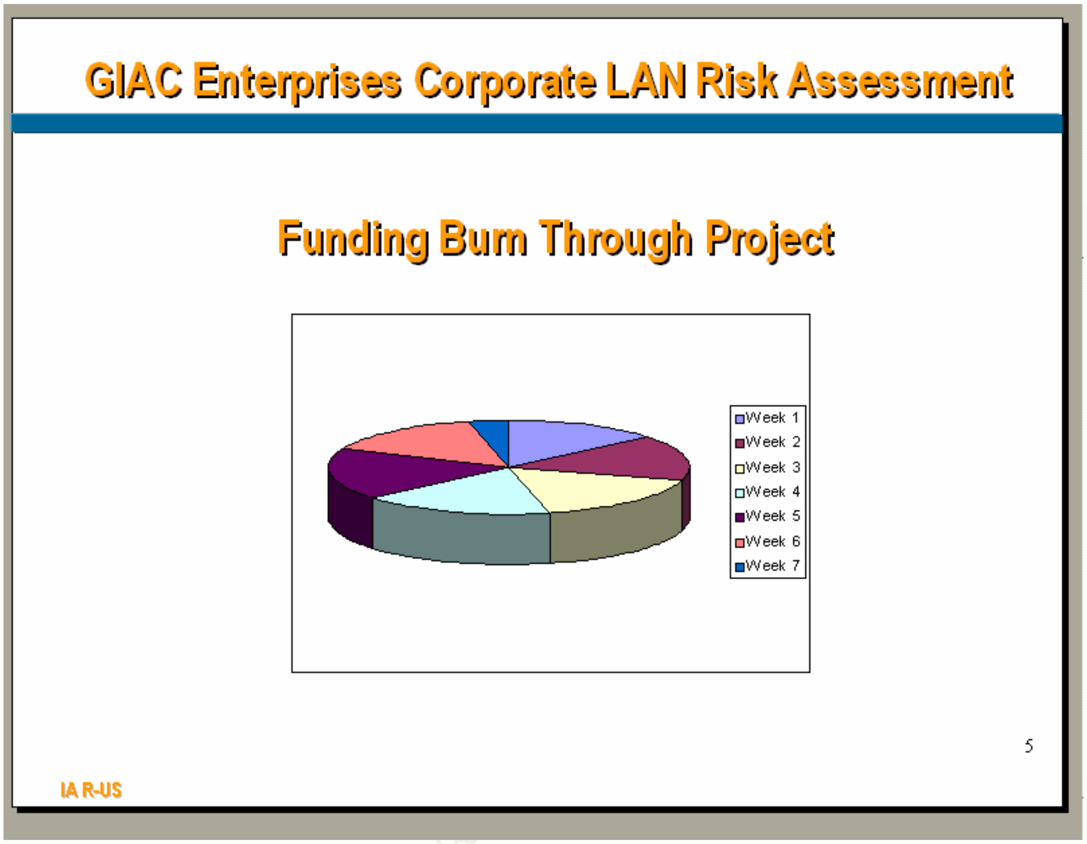
GIAC Enterprises Corporate LAN Risk Assessment

Initial POA&M

Actual POA&M

4

IA R-US

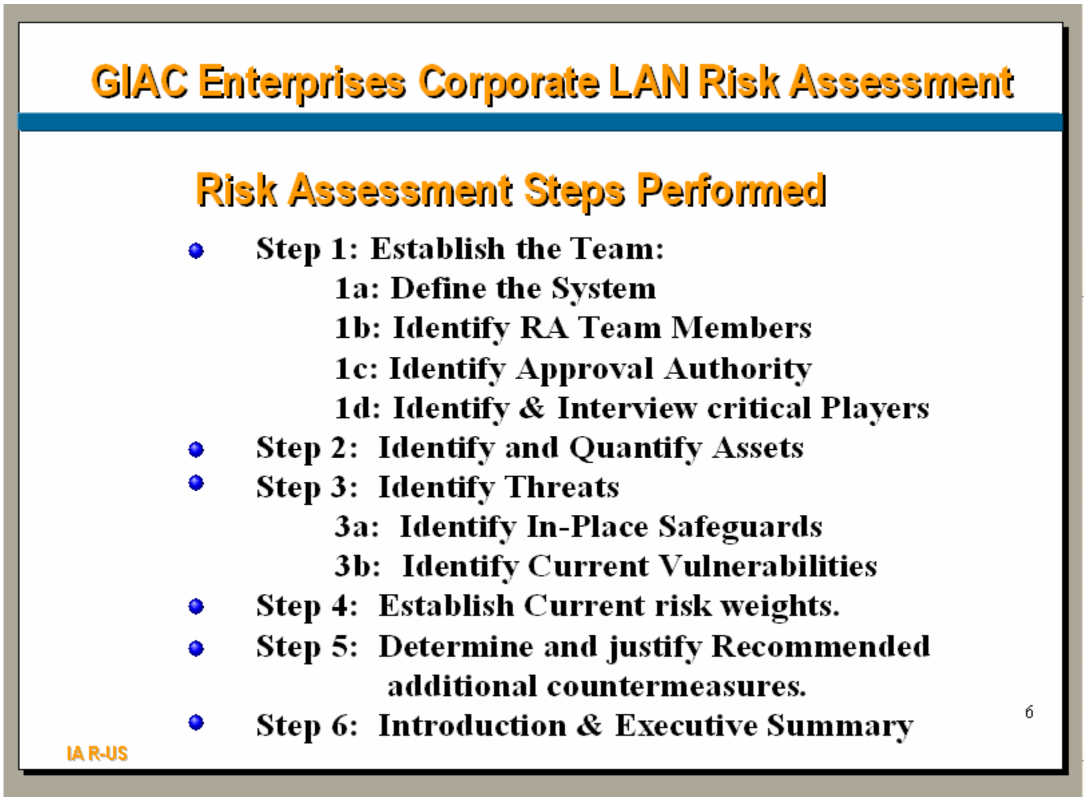


GIAC Enterprises Corporate LAN Risk Assessment

Funding Burn Through Project

5

IA R-US



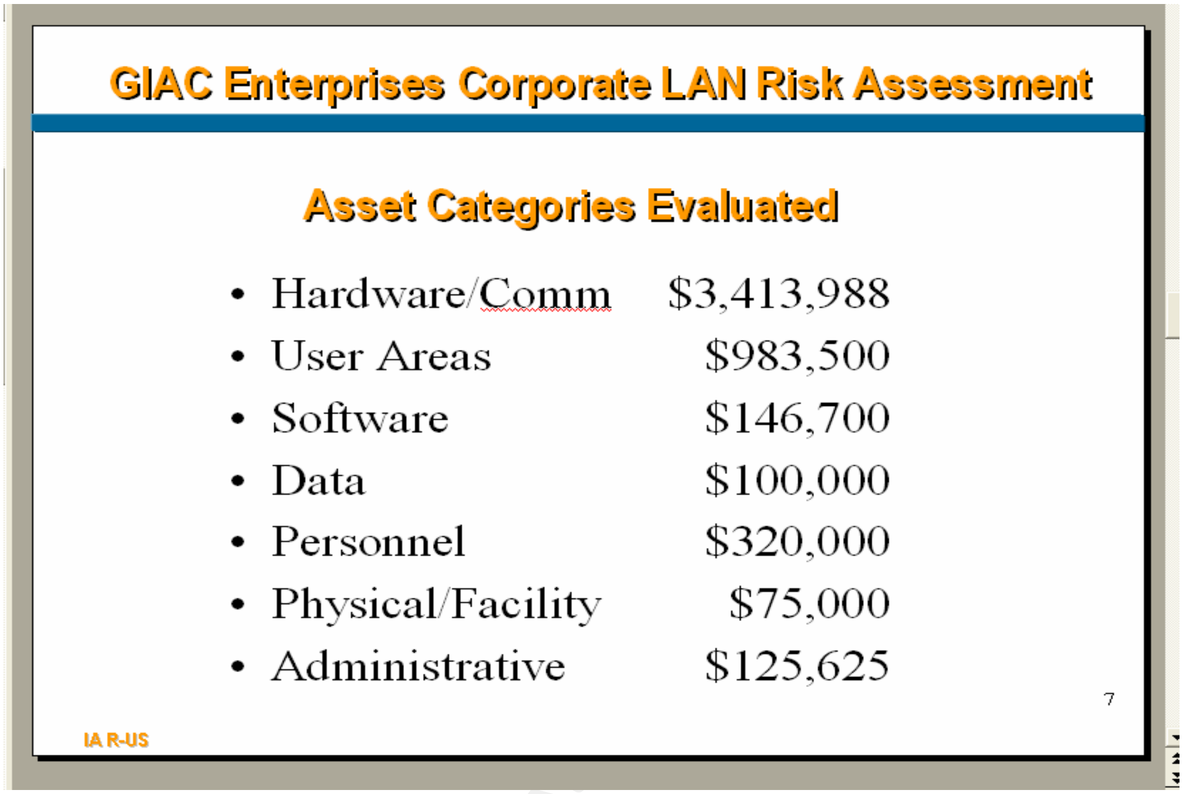
GIAC Enterprises Corporate LAN Risk Assessment

Risk Assessment Steps Performed

- Step 1: Establish the Team:
  - 1a: Define the System
  - 1b: Identify RA Team Members
  - 1c: Identify Approval Authority
  - 1d: Identify & Interview critical Players
- Step 2: Identify and Quantify Assets
- Step 3: Identify Threats
  - 3a: Identify In-Place Safeguards
  - 3b: Identify Current Vulnerabilities
- Step 4: Establish Current risk weights.
- Step 5: Determine and justify Recommended additional countermeasures.
- Step 6: Introduction & Executive Summary

6

IA R-US



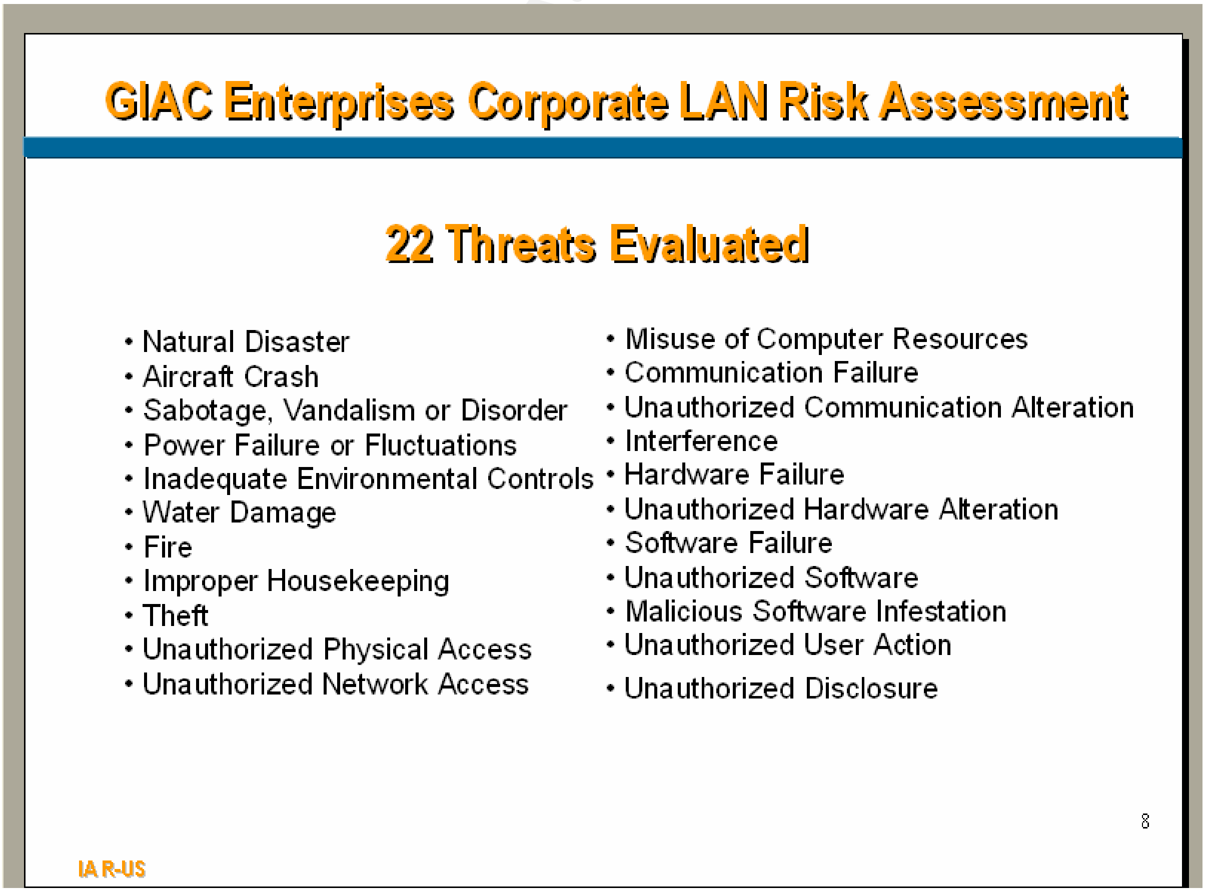
GIAC Enterprises Corporate LAN Risk Assessment

Asset Categories Evaluated

Hardware/Comm	$3,413,988
User Areas	$983,500
Software	$146,700
Data	$100,000
Personnel	$320,000
Physical/Facility	$75,000
Administrative	$125,625

7

IA R-US



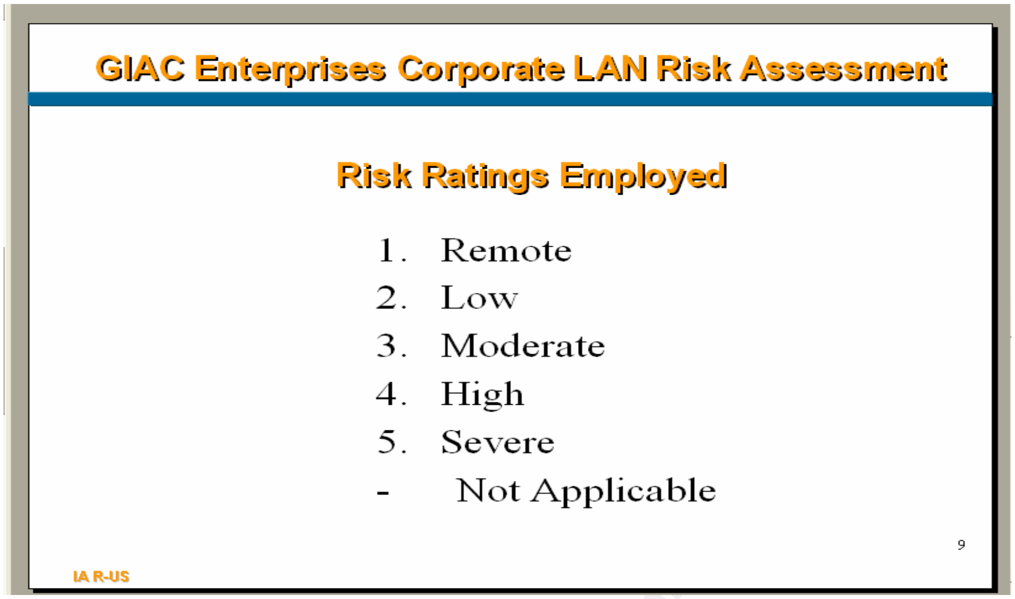
GIAC Enterprises Corporate LAN Risk Assessment

22 Threats Evaluated

- Natural Disaster
- Aircraft Crash
- Sabotage, Vandalism or Disorder
- Power Failure or Fluctuations
- Inadequate Environmental Controls
- Water Damage
- Fire
- Improper Housekeeping
- Theft
- Unauthorized Physical Access
- Unauthorized Network Access
- Misuse of Computer Resources
- Communication Failure
- Unauthorized Communication Alteration
- Interference
- Hardware Failure
- Unauthorized Hardware Alteration
- Software Failure
- Unauthorized Software
- Malicious Software Infestation
- Unauthorized User Action
- Unauthorized Disclosure

8

IA R-US



GIAC Enterprises Corporate LAN Risk Assessment

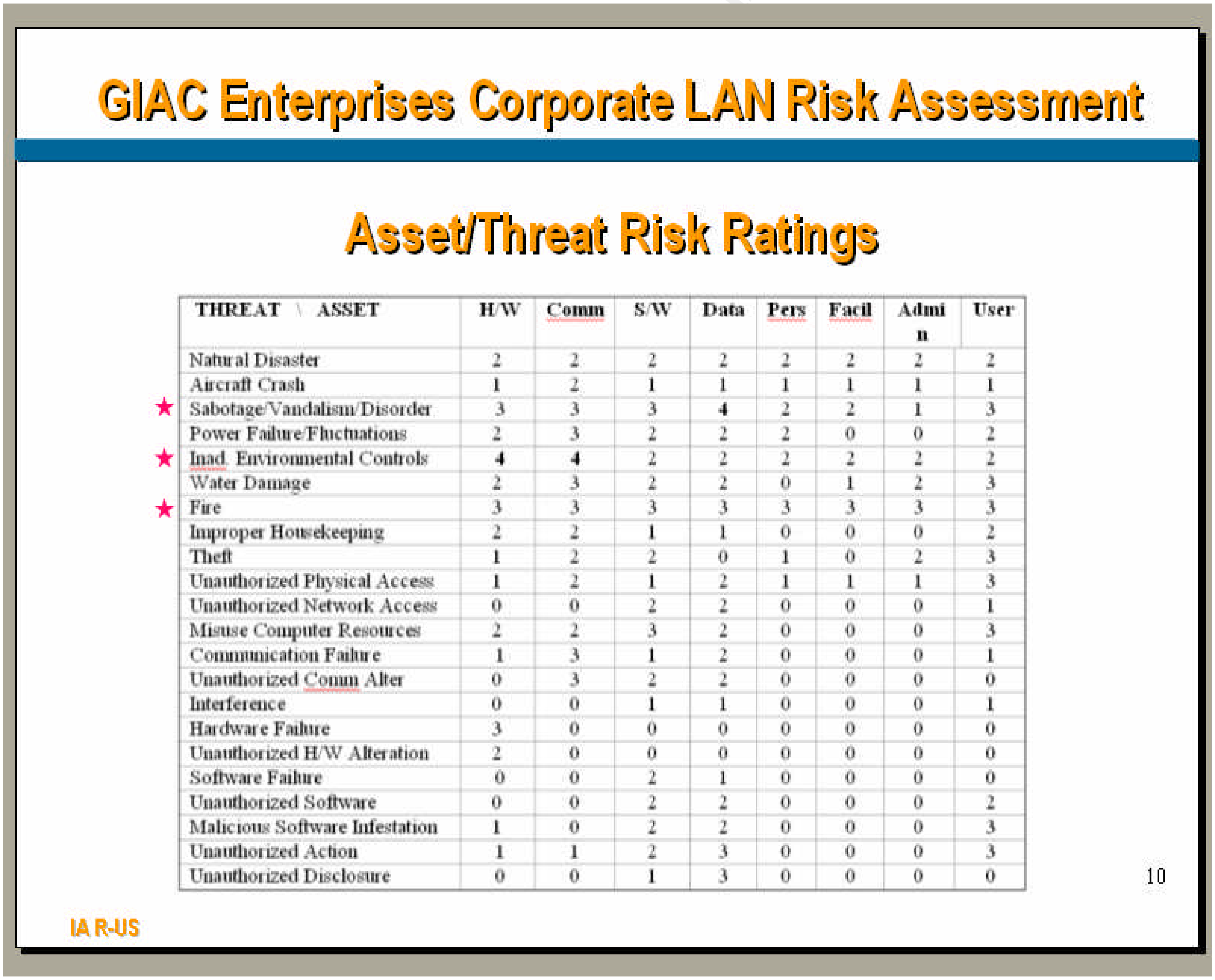
Risk Ratings Employed

1. Remote
2. Low
3. Moderate
4. High
5. Severe

- Not Applicable

9

IA R-US



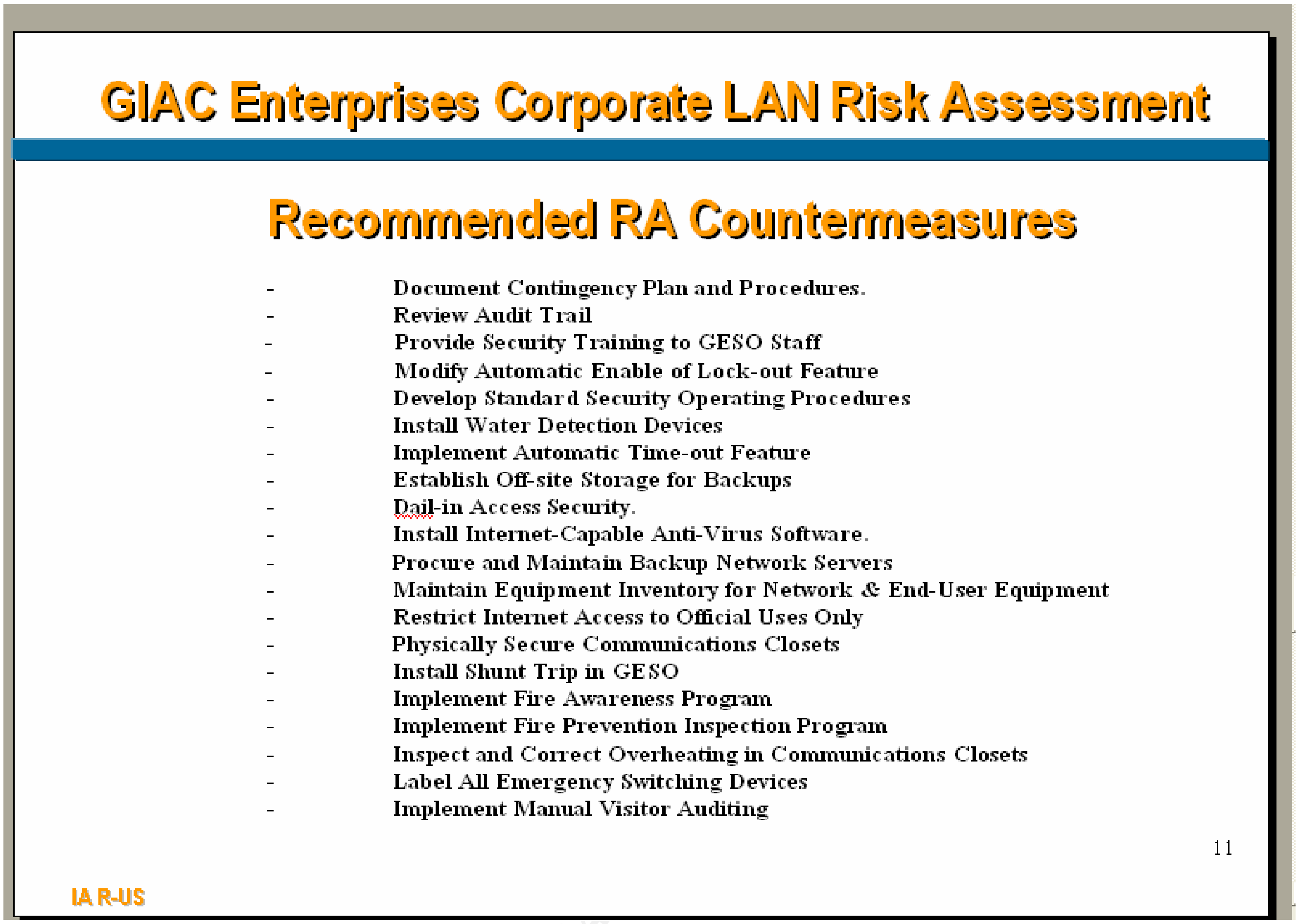
GIAC Enterprises Corporate LAN Risk Assessment

Asset/Threat Risk Ratings

THREAT \ ASSET	H/W	Comm	S/W	Data	Pers	Facil	Admi n	User
Natural Disaster	2	2	2	2	2	2	2	2
Aircraft Crash	1	2	1	1	1	1	1	1
★ Sabotage/Vandalism/Disorder	3	3	3	4	2	2	1	3
Power Failure/Fluctuations	2	3	2	2	2	0	0	2
★ Inad. Environmental Controls	4	4	2	2	2	2	2	2
Water Damage	2	3	2	2	0	1	2	3
★ Fire	3	3	3	3	3	3	3	3
Improper Housekeeping	2	2	1	1	0	0	0	2
Theft	1	2	2	0	1	0	2	3
Unauthorized Physical Access	1	2	1	2	1	1	1	3
Unauthorized Network Access	0	0	2	2	0	0	0	1
Misuse Computer Resources	2	2	3	2	0	0	0	3
Communication Failure	1	3	1	2	0	0	0	1
Unauthorized Comm Alter	0	3	2	2	0	0	0	0
Interference	0	0	1	1	0	0	0	1
Hardware Failure	3	0	0	0	0	0	0	0
Unauthorized H/W Alteration	2	0	0	0	0	0	0	0
Software Failure	0	0	2	1	0	0	0	0
Unauthorized Software	0	0	2	2	0	0	0	2
Malicious Software Infestation	1	0	2	2	0	0	0	3
Unauthorized Action	1	1	2	3	0	0	0	3
Unauthorized Disclosure	0	0	1	3	0	0	0	0

10

IA R-US



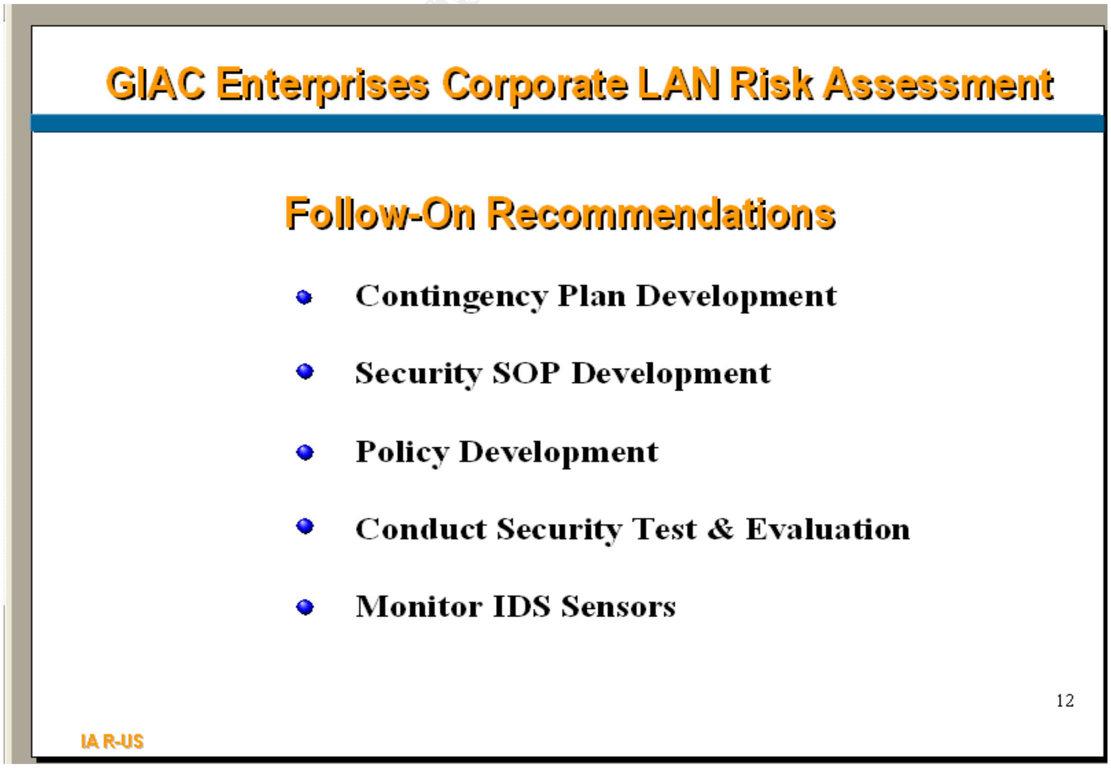
GIAC Enterprises Corporate LAN Risk Assessment

Recommended RA Countermeasures

- Document Contingency Plan and Procedures.
- Review Audit Trail
- Provide Security Training to GESO Staff
- Modify Automatic Enable of Lock-out Feature
- Develop Standard Security Operating Procedures
- Install Water Detection Devices
- Implement Automatic Time-out Feature
- Establish Off-site Storage for Backups
- Dail-in Access Security.
- Install Internet-Capable Anti-Virus Software.
- Procure and Maintain Backup Network Servers
- Maintain Equipment Inventory for Network & End-User Equipment
- Restrict Internet Access to Official Uses Only
- Physically Secure Communications Closets
- Install Shunt Trip in GESO
- Implement Fire Awareness Program
- Implement Fire Prevention Inspection Program
- Inspect and Correct Overheating in Communications Closets
- Label All Emergency Switching Devices
- Implement Manual Visitor Auditing

11

IA R-US



GIAC Enterprises Corporate LAN Risk Assessment

Follow-On Recommendations

- Contingency Plan Development
- Security SOP Development
- Policy Development
- Conduct Security Test & Evaluation
- Monitor IDS Sensors

12

IA R-US