Version FINAL

August 2011

Red Team Report
CleanSweep: Technical Details

Prepared for: **United States Department of Labor**
Mr. Ed Hugler
Deputy Assistant Secretary for Operations
United States Department of Labor
Frances Perkins Building
200 Constitution Avenue
Washington, DC

Prepared by: Scott Maruoka
RT Project Lead
Department 5627
San[redacted]al Laboratories
505-
P O Box 5800, MS 0620
Albuquerque NM 87185-0671

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

For additional Information, contact:
Han Wei Li[redacted], Project Manager
Phone[redacted]

IDART™
Information Design Assurance Red Team

National Nuclear Security Administration

Sandia National Laboratories

Table of Contents

Executive Summary

Over the course of the last four years, the DOL was approached by various regulatory authorities (e.g. OIG, SEC, and FBI) concerned that key economic data were potentially subject to unauthorized, premature release.

The economic data in question are subject to an embargo process whereby DOL controls the timing of its release to reporters and the general public. The objective for CleanSweep was to identify potential vulnerabilities in the DOL Press Lockup room facility and associated data embargo and release procedures, provide mitigation options for vulnerabilities identified, and assist in mitigation verification should DOL decide to implement recommended mitigation options.

CleanSweep customers included stakeholders from several organizations within DOL: Operations, the Office of Public Affairs (OPA), and the Bureau of Labor Statistics (BLS). Each of these entities had its own unique perspective regarding the nature of the perceived threat and consequently, differing ideas on potential solutions. The common concern amongst these stakeholders revolved around the unauthorized, premature release of embargoed data.

Likely adversaries in this scenario are profit-driven, technically sophisticated individuals who may have considerable resources at their disposal. Their technical proficiency enables implementation of stealthy surveillance equipment. Though they are willing to bend and potentially violate rules and laws, violence is unlikely as an operational method.

Though DOL, BLS, and OPA personnel are doing due diligence in their efforts to monitor the press lockup facility, their efforts are complicated by the presence of non-DOL IT equipment and communications lines in this facility. The opaque nature of this equipment to DOL, BLS, and OPA stakeholders is a major impediment to ensuring that embargoed data is not released prior to authorization.

The presence of equipment owned by press organizations necessitates that access to areas housing DOL communications and data infrastructure is made available to contractors working for these press organizations to conduct maintenance. This access, though controlled by DOL personnel escorting such maintenance contractors, creates opportunities for adversaries to compromise critical DOL communications and data infrastructure.

The following actions would mitigate against risks identified during CleanSweep:

- Replace computers and other IT equipment in the Press lockup facility with DOL owned equipment and remove the private data lines currently in use. This would eliminate the need for the Black Boxes altogether.
- Prohibit anyone other than DOL personnel (or contractors working *for* DOL) from entering communications closets without a technically knowledgeable escort.
- Provide/train technically knowledgeable escorts.
- Modify existing policy to require personal items be kept in lockers ***outside*** of the Press Lockup room. Divestment should be a prerequisite for room entry.

Though not directly addressed in the SNL Red Team analysis, the apparent root cause for the issues driving this assessment is the presence of algorithmic traders in the press lockup facility. Modifying DOL policy on what criteria qualifies applicants to attend release events would likely be of benefit.

CleanSweep: Technical Details

This section of the report is intended for personnel interested in the details of the Sandia Red Team conclusions described in the Management Overview. Some of the information is repeated from previous sections to help establish context for those readers who have chosen to begin with this section. Where that information is repeated, additional detail is provided for the technical reader.

Introduction

Over the course of the last four years, the DOL was approached by various regulatory authorities (e.g. OIG, SEC, and FBI) concerned that key economic data were potentially subject to unauthorized, premature release. The economic data in question are subject to an embargo process whereby DOL controls the timing of its release to reporters and the general public. The focus of DOL management concern is the physical, technical, and procedural controls which constitute this embargo process.

Objective

SNL IDART was tasked to identify potential vulnerabilities in DOL press lockup room facilities and associated data embargo and release procedures, provide mitigation options for vulnerabilities identified, and assist in mitigation verification should DOL decide to implement recommended mitigation options.

Information sharing was performed via SNL external SharePoint (an SSL-enabled collaboration application).

Sandia's IDART team executed the following assessment activities:

1) Document Review- Analysis of available security processes, procedures, rules, security equipment technical specifications, floor plans, and other artifacts relating to the embargo process. Conduct open source research on pertinent subjects.
2) Kickoff meeting- Face-to-face engagement with key stakeholders in the embargo process to set common expectations for the assessment outcome, and finalize scope and the rules of engagement for assessment activities.
3) Vulnerability Assessment- IDART Team members conducted an inspection and evaluation of the physical attributes of the press lockup facility and surrounding areas within the Frances Perkins Building, the information technology equipment contained within the Lockup Facility, associated communications infrastructure, technical security equipment, and conducted interviews with DOL personnel tasked with implementing the embargo process.
4) Sandia National Laboratories technical specialists executed exterior and interior surveys of the radio frequency (RF) spectrum in the area of interest, and conducted another radio frequency spectrum analysis during an information embargo/release event. These personnel used a combination of proprietary and publicly available but controlled equipment and applications.

a. Establish baseline RF readings for the target area.

b. Conduct RF assessment of the target area during a press event.

c. Compare results, identify anomalies.

Findings from these assessment activities were analyzed using the IDART methodology described throughout this document, and the results are recorded in this report.

Rules of Engagement

SNL IDART actions were limited to observation and assessment during CleanSweep- no attempts were made to actively exploit potential vulnerabilities identified. DOL agreed to provide access and support to SNL IDART team members during assessment activities. These Rules of Engagement (ROE) were developed by SNL IDART personnel in concert with DOL officials, and were formulated to ensure that the Red Team assessment activities would not adversely impact DOL operations while concurrently providing results useful to DOL management for formulating risk-based corrective measures, if needed.

Of particular note is that IT systems (e.g. computers, monitors, I/O devices, routers, switches) within the press lockup facility are not owned by DOL, with the exception of the AirPatrol console and LAN. Each press agency with access to the lockup facility owns and maintains their own equipment, including the communications lines to the outside world. The SNL IDART Red Team was therefore limited to visual examination (no physical contact) and observation (visual and passive RF) when the systems were used by press personnel during a press release.

Notification: Sandia presented proposed assessment activities for CleanSweep to DOL officials in the Statement of Work (SOW) created prior to commencement of this project. Approval of the CleanSweep SOW signified DOL approval for the assessment activities documented therein. SNL agreed to notify DOL officials prior to the start of any assessment activity and obtain DOL approval before beginning any such activity. Sandia will notify DOL at the conclusion of the assessment and verbally provide the results. SNL IDART and DOL personnel worked jointly to develop the assessment schedule of activities, providing concurrence on assessment dates, times, and processes.

DOL officials were made aware of and consented to the requirement that federal law enforcement be notified should SNL IDART personnel discover surveillance devices during their assessment.

Information Protection: Information collected during the course of CleanSweep will be retained by Sandia in electronic work papers. A final report that includes notifications of findings, recommendations that summarize preliminary findings based on these data, and possible remediation actions for information technology security weaknesses or deficiencies will be provided to DOL officials at a results briefing. Sandia will destroy all retained copies of logs and data at the request of DOL.

Technical Details of this Sandia assessment report contains Official Use Only information describing specific vulnerabilities and attack steps for potential exploits. No classified

information was generated during the course of CleanSweep activities. Sandia will protect all copies of logs and data appropriate to the level of sensitivity. All SNL IDART personnel agreed to protect and hold in confidence any DOL proprietary information discovered during the course of CleanSweep, and provided written assent of this agreement to DOL officials.

Scope

Ideally, Red Teams would prefer to identify every weakness in a target system, explore and test all vulnerabilities, and produce a report providing a complete picture of the target environment's security posture. In reality, a project's budget and schedule place a limit on the scope of assessment activities.

The IDART process adds further limits to project scope by specifying the threat model and associated adversaries and constraints. These limits are used as "reality checks" on Red Team courses of action and recommendations. For DOL, the threat model originally specified an adversarial upper limit of "moderate capability", characterized by individuals or organizations seeking to profit from premature access to embargoed economic data. As explained by officials representing the Department of Labor, the Office of Public Affairs (OPA), and Bureau of Labor Statistics (BLS), the scope of this assessment was limited to how such an adversary might exfiltrate embargoed economic data from the press lockup facility during a press release event.

The Red Team concentrated on the following:

- Physical attributes of the press lockup facility and surrounding areas within the Frances Perkins Building, 200 Constitution Avenue NW, Washington, DC.
- Business processes associated with press embargo and release procedures as documented by policy, and as observed during an actual press release event
- Radio Frequency (RF) environment for the area of interest
- Computer and communications equipment in the press lockup facility
- Communications infrastructure for the press lockup facility

The Red Team specifically did not consider the following:

- Threats and vulnerabilities associated with DOL insiders
- Threats and vulnerabilities associated with DOL Information Technology (IT) systems used in the acquisition of data and production of finished economic analysis
- Surveillance vulnerabilities at other locations associated with the data embargo and release process
- Parallel embargo/release facility and process for television journalists

Red Team

Sandia/IDART created a team whose members possess skills specifically chosen to address the various issues presented by this project, with Red Team members representing several Sandia organizations. The team consisted of five (5) members with

technical specialties including cyber security and threat assessment, IT system penetration and exploitation, physical security design and threat assessment, electronic surveillance, and risk management.

Analysis Environment

All CleanSweep activities occurred at the United States Department of Labor headquarters, located in the Frances Perkins Building at 200 Constitution Avenue, Washington, DC as depicted in Figure 1. The six story steel and limestone building covers two square blocks near the base of Capitol Hill, and was completed in 1974.[1]

Figure 1. Frances Perkins Building exterior view from Constitution Avenue.

The IDART Red Team conducted preliminary analysis of information acquired during this assessment while on site, which was communicated to DOL stakeholders during an out-briefing at the conclusion of assessment activities. A copy of the CleanSweep agenda is provided as Attachment A.

Upon returning to the Sandia National Laboratories Albuquerque, NM facility the Red Team and an IDART subject matter expert (who did not accompany the Red Team to DOL), conducted further analysis to identify and then refine potential attack scenarios and appropriate mitigation strategies.

Methodology

For this assessment, the Red Team used the IDART methodology illustrated in Figure 2. The IDART methodology follows the standard activities shown on the left of the figure by performing the work and developing the products shown on the right of the figure.

IDART allows a red team to tailor a mature, repeatable assessment framework to the needs of a customer and the budgetary and scheduling realities of a project. We accept that complete understanding of a highly complex system is impractical for most projects and we use the IDART process to generate meaningful assumptions and realistic simplifying representations for the target system. This approach allows us to capture the principal features and generate custom viewpoints that are used to understand processes and interactions and to identify critical interfaces and components. Combining this understanding with domain expert knowledge, we can then identify system and subsystem vulnerabilities and predict their effect on both system components and the system as a whole.

Note that the maturity of the target system affects the applicability of the IDART process. A system must have a reasonable level of maturity—be it in the operational or design phase—in order to support an IDART methodology assessment. According to information provided by DOL, OPA, and BLS officials during interviews and background documentation obtained during data collection and review, the press lockup process is a well-established and important component of the DOL mission.

The first four phases of the IDART process are described in detail in the following sections. Each section starts with a description, followed by a summary of what was actually performed for the DOL CleanSweep assessment. The last two phases "Reports" and "Demos & Experiments," have been rolled up into the results section at the end.

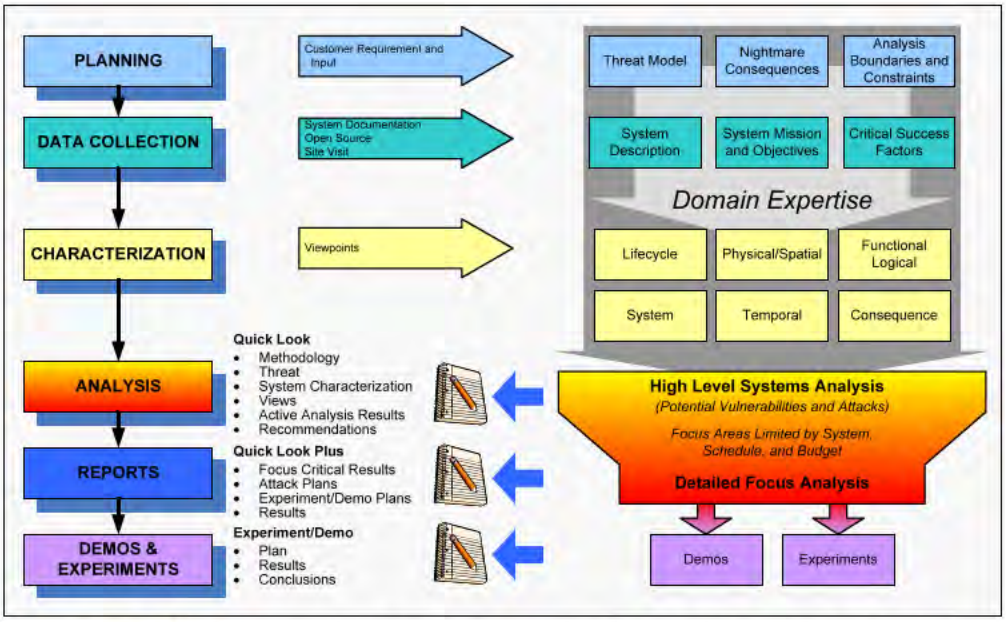

Figure 2: IDART Methodology. Phases depicted to the left consist of tasks/activities (shown as arrows) resulting in products and deliverables typically coalesced and documented in a final report.

Planning

In the "Planning" phase, the Red Team identifies the adversary and capabilities that will be modeled, the worst case scenarios for system failure, and any constraints that will be

placed on the analysis or on the Red Team. The results of this phase are based on customer requirements and are usually produced by a joint Red Team/customer team, although sometimes the Red Team develops recommendations that are submitted to the customer for approval.

DOL officials and SNL management team members conducted initial discussions on the issue of a potential information leak of sensitive economic data during the embargo and release process, resulting in a preliminary site visit by SNL personnel. Subsequently, SNL IDART Project Manager, Han Lin, and Project Lead, Scott Maruoka, worked with DOL officials to create a Statement of Work (SOW) capturing and documenting project details regarding perceived threat, nightmare scenarios, associated milestones and deliverables, and project scope and constraints to IDART activities.

Data Collection

The second phase of the IDART Methodology consists of data collection. In this phase, the Red Team reviews all available applicable documentation, collects open source material relevant to the target system, and visits an operational customer site if feasible and appropriate. This phase serves to provide the Red Team with the appropriate background information to model the adversaries identified in the Threat Model. The Red Team develops a detailed description along with the mission and objectives of the target system. The Red Team also identifies its critical success factors—a list of objectives that will serve as indicators of Red Team success. The subsequent system characterization and analysis phases are very dependent on the accuracy and completeness of the system description generated in this step. As noted previously, IDART activities were limited to observation and assessment during CleanSweep so success indicators were not applicable as no penetration and exploit tests were conducted.

CleanSweep data collection activities consisted of document review, interviews of DOL Operations, OPA, and BLS personnel, physical inspection of the press lockup facility and adjoining areas, wiring closets and telecommunications hub rooms, and observation of a live press event involving data embargo and release.

DOL provided the following data:

1) DOL Lockup Room Wireless Device Detection User Guide- combined concept of operations (CONOP) covers Air Patrol console, Mantis Handheld Bluetooth detector, and AirCheck Wi-Fi tester equipment.
2) DOL Lockup Room Task Summary- step-by-step CONOP covering Air Patrol, AirCheck, and Mantis tools.
3) Press Room Activity logs- 10 JAN 2011 – 12 APR 2011- chronologically ordered documentation of Press Lockup facility monitoring activities performed by BLS Information Assurance personnel; sample report form.
4) Black Box user's manual and technical specifications.
5) Equipment to Black Box Cabling guide.

6) Inventory of Black Boxes in use.
7) A Hall/Fillichio memo dated March 2, 2011 suggesting various changes to security policy and procedures for the Press Lockup facility.
8) Evacuation and shelter in place policy for the Press Lockup facility.
9) A draft copy of Lockup facility rules for press personnel and their employers.
10) A draft copy of Lockup facility responsibilities for DOL staff.
11) Numerous photographs of the Press Lockup facility work spaces.
12) Floor plans for the Frances Perkins building and the Press Lockup facility.
13) Findings from previous assessments conducted by BLS IA.
14) Timeline of security issues and associated mitigation measure implementation.
15) May 2008 letter from OPA to news organizations documenting security rules for the Press Lockup facility.
16) Meeting minutes from 2008 incident response.

Characterization

During system characterization, the Red Team combines all the inputs from the Planning and Data Collection phases with domain expertise to generate a variety of different viewpoints, such as those listed in the IDART Methodology diagram. Some viewpoints may be simple as vendor-supplied network maps or physical diagrams. Others may show complex timing interactions between system components and external input sources.

Temporal View

Based on interviews of OPA and BLS personnel and first-hand observation, SNL IDART produced the temporal view illustrated in Figure 3, Data Embargo and Release timeline.

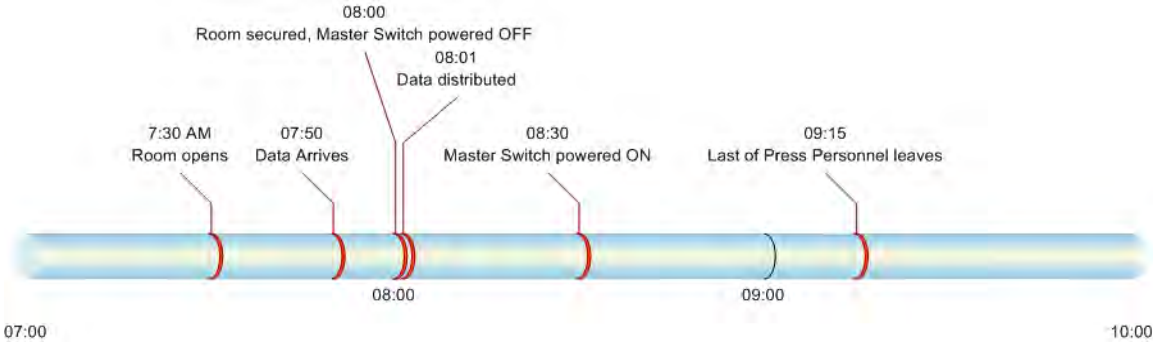

Figure 3. Data Embargo and Release timeline.

SNL IDART personnel noted that press attendees queued up outside the press lockup facility waiting for the room to open. Once allowed in, these press personnel dispersed to their various work areas. Sign in and surrender of cell phones occurred after they had been allowed entry, with some individuals needing to be reminded by OPA personnel to sign in and turn in cell phones. Requiring press to sign in and surrender cell phones prior

to Lockup facility entry would facilitate control and lessen the likelihood that press may forget to follow the rules.

Physical Views

The area around the Frances Perkins Building is heavily developed, with neighboring structures occupied by a mix of government, commercial, and non-profit entities. Figure 4 depicts an aerial view showing the structure and surrounding area, while Figure 5 depicts a floor plan of the 1st floor with the press lockup facility highlighted.

Figure 4. Frances Perkins Building (center), aerial view. [redacted]

[redacted]

Figure 5. Frances Perkins building floor plan with press lockup facility highlighted.

Access to the Frances Perkins building is controlled by a security force and checkpoints consisting of metal detection and x-ray screening equipment. Press personnel are issued special identification credentials (badges) worn to be visible to security force personnel. These badges allow press personnel to pass an internal security checkpoint consisting of a security guard (no x-ray or metal detection equipment) controlling access to the press lockup facility and surrounding area. During assessment activities, SNL IDART personnel noted that individuals wearing press badge credentials had unescorted access to upper floors of the building as well as the press lockup facility and immediate area.

While examining the area used by television journalists, SNL IDART personnel noted an exterior access door was propped open by a cameraman to facilitate equipment movement between the exterior taping location and the building interior. No security personnel were within line-of-sight.

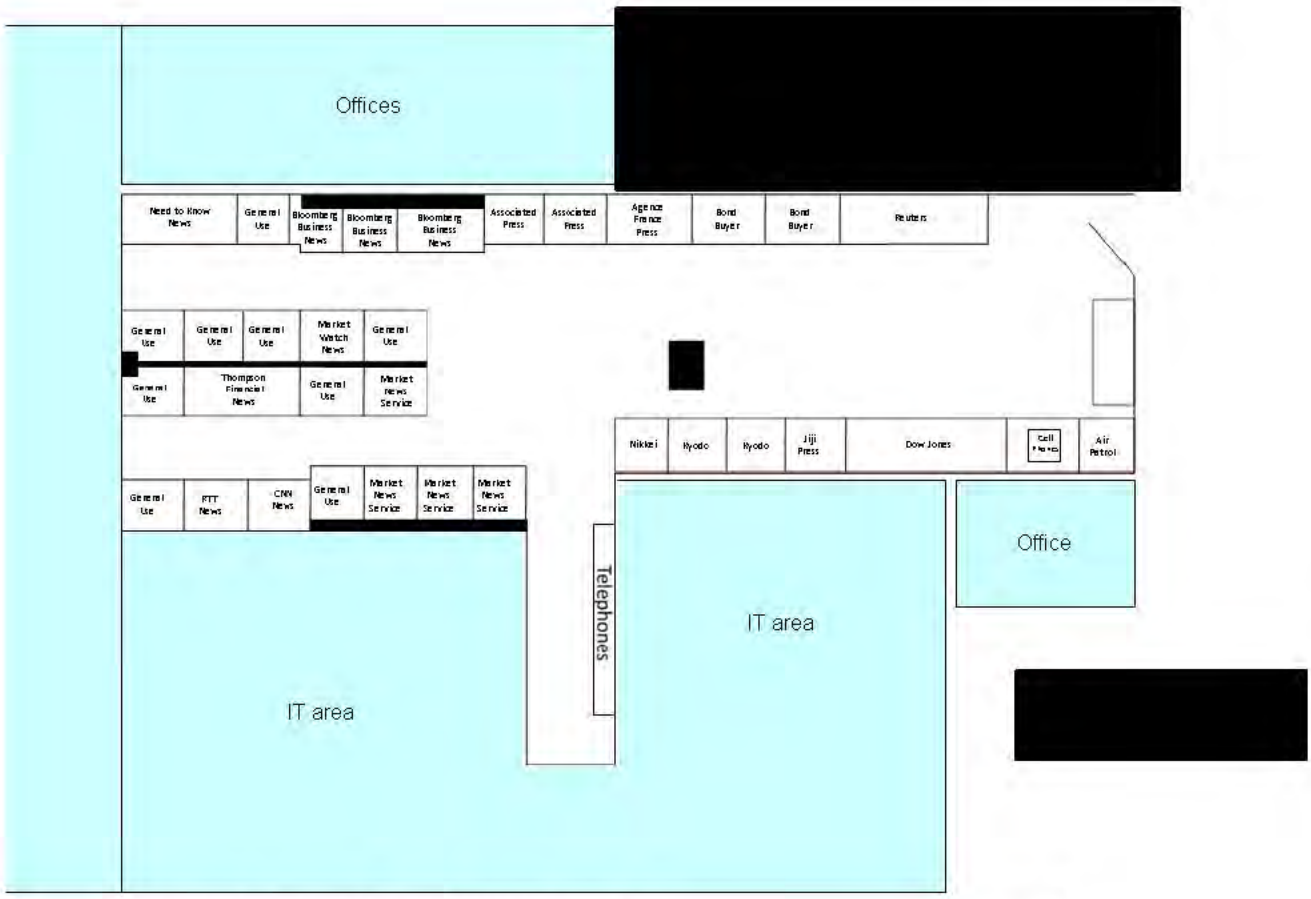

Figure 6. Press lockup facility and adjoining areas. [redacted]

According to a DOL employee, members of the general public are issued visitor badges upon surrendering a picture ID at the security checkpoints. [redacted]

[redacted] A storage area and HVAC equipment and associated ducts lie below. This basement is not accessible by the general public.

Figure 7. Cluttered press work area, showing what appear to be networking appliances to the left of the workstation and monitor. Note the two Black Boxes atop the network gear.

The interior of the press lockup facility is somewhat crowded, and some of the work spaces used by press personnel are cluttered with IT equipment, as illustrated by Figures 7 and 8. Members of the SNL Red Team were somewhat surprised to find what appeared to be network appliances (e.g. switches and routers) capable of supporting infrastructure well beyond the workstations to which they were connected. Since these devices are not DOL-owned equipment, the Red Team was limited to visual-only inspection, and could not verify that computer and network appliance cases and chassis contained only standard equipment. As explained by OPA and BLS staff, the elaborate networking configurations are meant to give their owners an advantage over neighboring competitors in transmitting data when it is authorized for release.

During the live press release event, IDART personnel in the press lockup facility noted the ambient temperature became uncomfortably warm, likely due to the human occupants and the considerable amount of IT equipment present. Many of the work areas featured more than one Black Box, which are supplied by DOL.

Figure 8. Cluttered press work area, with Black Box under network appliance and obscured by telephone.

RF View

SNL technical personnel conducted external and in-conference inspections of the Radio Frequency (RF) environment both prior to and during a live press release, to detect the presence of clandestine surveillance devices in the area. No such devices were detected. A breakdown of these activities consisted of:

1) Search and analysis of the RF spectrum in the target area delineated as the press lockup facility. See Figure 9.
2) Technical and physical examination of fixtures, furnishings, and equipment located within the target area.
3) Technical and physical examination of electronic and electrical equipment, electrical wiring, and utility pathways.
4) Technical and physical inspection of the interior and exterior surfaces of the perimeter walls, floors, ceilings, and other structural objects within the target area.
5) Physical inspection of the exterior perimeter to include applicable spaces above and below the target area.

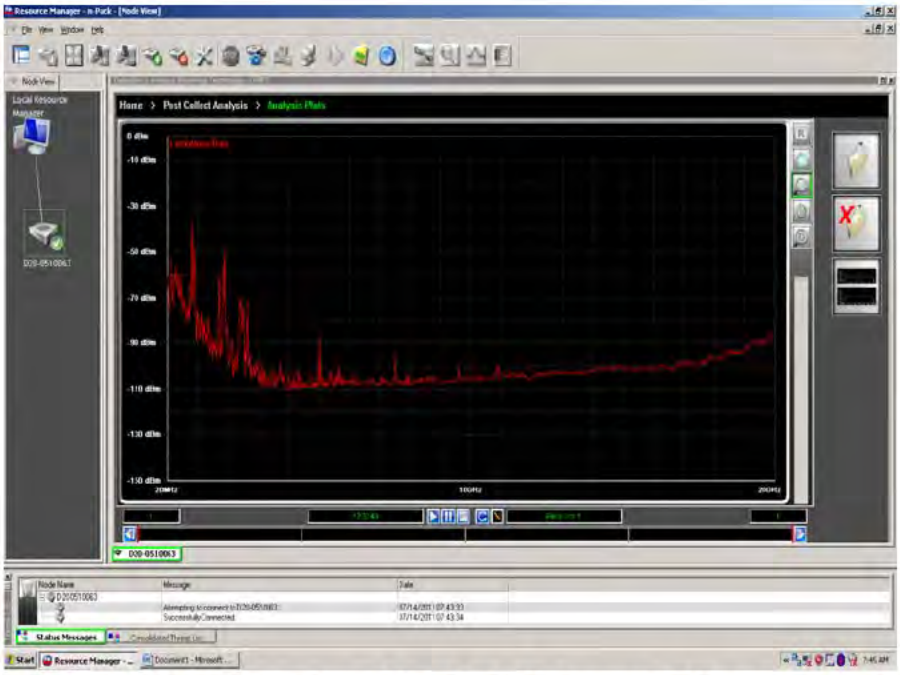

Figure 9. High level overview of the Radio Frequency (RF) spectrum. Currently displaying from 20MHz up to 20GHz. The "peaks" are common high use areas of the spectrum.

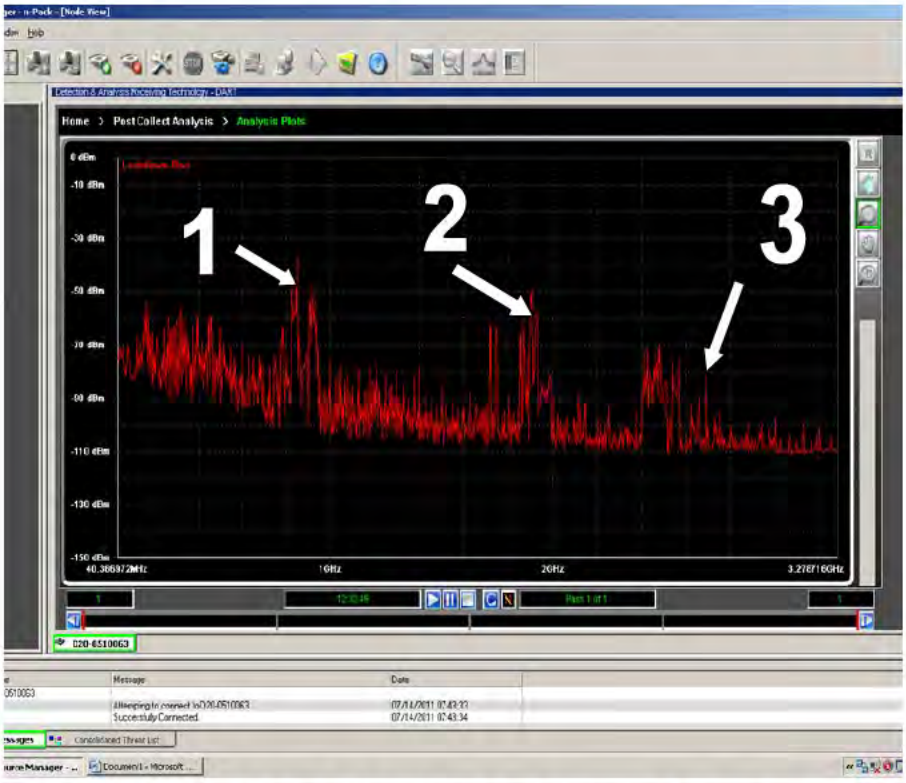

Figure 10. Zoomed in view of high use and common frequency ranges. It's expected to see activity in these areas. 1 - 850MHz – Cellular band; 2 - 1800Mhz – Cellular band; 3 – 2.4GHz – Wireless (WiFi) band.

For RF monitoring during the press release, SNL technical personnel set up equipment in an office adjacent to the target area, with a BLS IA representative observing. An RF contact observed during the press release event was determined to have been caused by a source outside the Lockup facility, and was also identified by BLS IA personnel on their equipment.

Analysis

The Analysis phase is highly variable, depending on the project's budget and schedule, the Threat Model, and any constraints identified during the Planning phase. This phase can range from a Quick Look overview (as was conducted for CleanSweep), which identifies potential vulnerabilities and attacks without verification testing, to a detailed analysis in which the system or portions of it are subjected to a deep analysis with full attack development, validation, and countermeasure generation.

The intentionally limited scope and rules of engagement for CleanSweep dictated that no penetration testing and exploitation of identified vulnerabilities occur. Based upon information derived from document review, interviews, and direct observation on site, the Red Team conducted a tabletop attack brainstorm exercise resulting in attack graphs depicting potential attacks that team members thought had viable potential for success.

Threat Model

The IDART methodology begins by developing a threat model to be used for Red Team operations. As the scope of operations for CleanSweep was limited to observation and analysis, no attack exercises were conducted. Instead, threat and adversary modeling provided the basis for attack scenario vetting- what was realistic in terms of perceived attacker goals and capability limitations. This model defines the adversaries along with their skills, resources, and motivations. Establishing an adversary model allows analysts to postulate more accurately on what types of attack tools or weapons will likely be brought to bear against defenders, and so instruct as to the most appropriate mitigation strategies to employ.

Threats

The first step in developing a threat model is to establish which threats exist to the target system’s mission and which threats the target system is intended to mitigate. Figure 11 shows general system threats as they relate to operational environments.

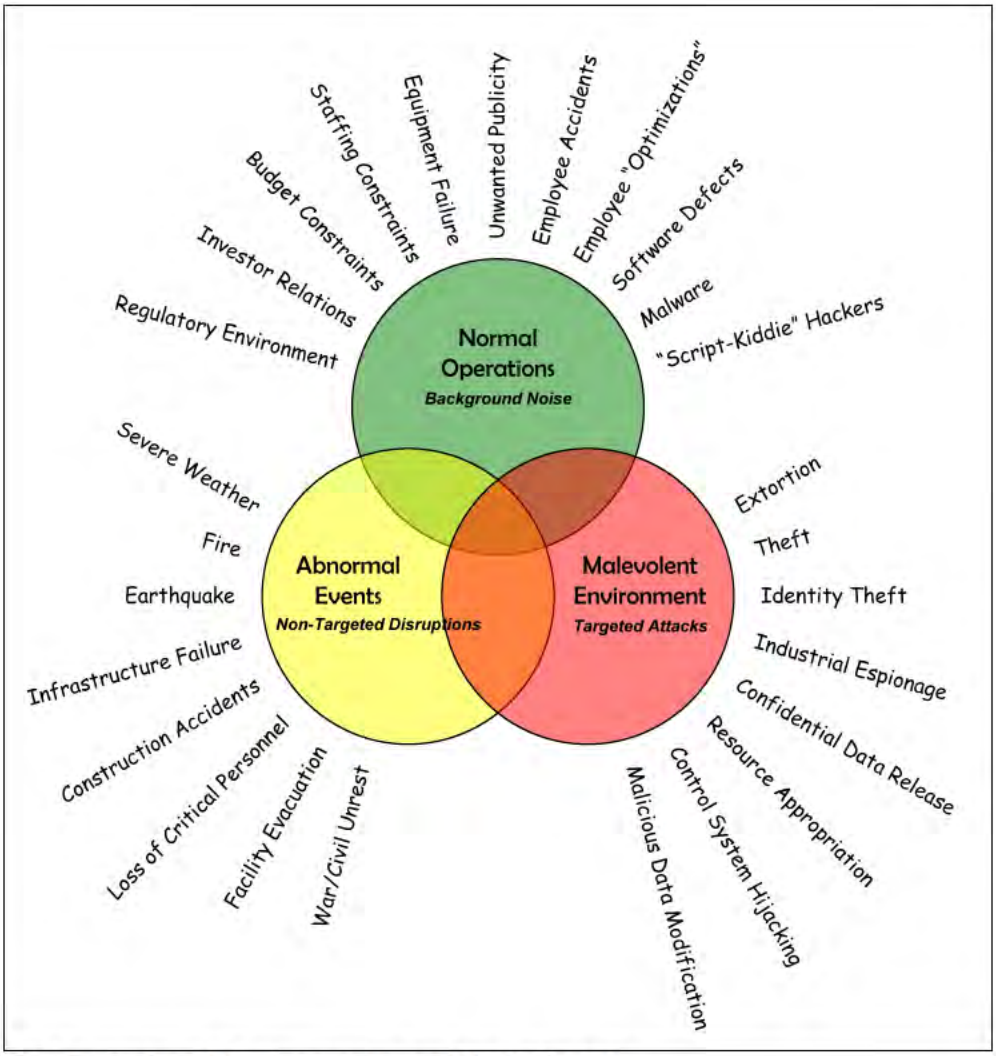

Figure 11: Operational Environments and Their Threats.

Sandia's threat model identifies three operational environments:

- Normal Operations: This includes everyday events in a benign operational environment. No exceptional disruption or targeted attack is occurring and threats are limited to those that are expected in day-to-day operations. Note that we include malware (worms and viruses) as well as script-kiddie-type hacker actions, as they are now part of the background noise to which most computer systems and networks are continuously subjected.
- Abnormal Events: These include disruption threats that are not specifically targeted at the system. Environmental threats such as severe weather and fire are good examples. An organization will often have a recovery plan that enumerates the steps necessary to recover from these events, to resume operations albeit in a contingency mode.
- Malevolent Environment: The malevolent environment includes actions that target the system specifically. These are malicious, intentional attacks designed specifically to harm or exploit the target system either directly or indirectly.

Although we consider and analyze threats in normal operations and abnormal events, Sandia's Red Team and IDART process concentrate on the malevolent environment.

The maturity of the target system determines how far into the malevolent environment the Red Team plays. Some systems are in a state in which they cannot operate successfully in a normal operational environment; thus it makes no sense for the Red Team to represent sophisticated malevolent threats. Other systems may have been red teamed before and are in a much more mature state in which they are ready to take on malevolent adversaries. Figure 12 shows this relationship.

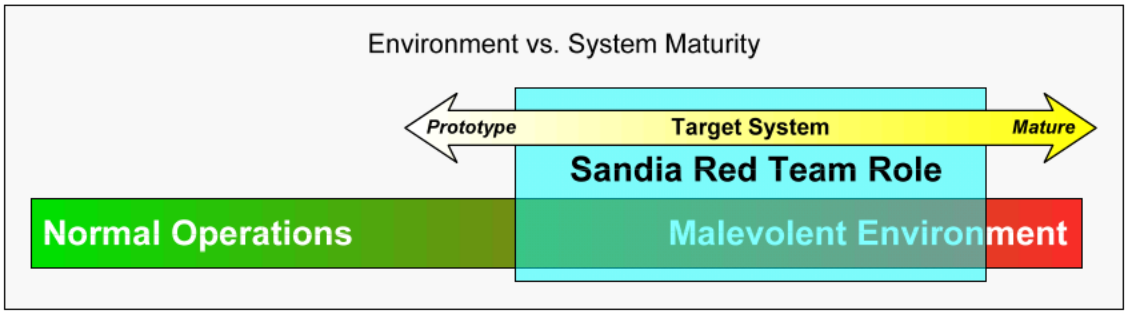

Figure 12: Red Team Role Based on System Maturity.

Nightmare Consequences

Nightmare consequences are worst-case scenarios involving compromise or misuse of information and perhaps the systems which produce and/or store such. In the formal IDART methodology, these consequences are mission oriented- how will compromise of information and associated IT systems adversely impact the target organization's mission, its ability to do business? After nightmare consequences are identified, the Red Team attempts to find a way to simulate them within the limitations of the identified adversary's capabilities. Since CleanSweep activities were limited to assessment and observation, simulations were necessarily limited to tabletop exercises.

CleanSweep customers included stakeholders from DOL Operations, the DOL Office of Public Affairs (OPA), and the Bureau of Labor Statistics (BLS). Each of these entities had its own unique perspective regarding the nature of the perceived threat and consequently, differing ideas on potential solutions. The common concern amongst these stakeholders revolved around the unauthorized, premature release of embargoed data.

Nightmare Consequences for CleanSweep Stakeholders

- All- Scandal- data leak results in negative press, loss of reputation
- OPA- Algorithmic traders subvert press release process, supplant "real" journalists
- BLS- Loss of "gold standard" reputation for fairness and accuracy

Adversary

Sandia has developed detailed models that identify the skill, resources, motivations and threats of various adversaries. That said, these models can rarely be simply plugged into a project. Since every system that a red team assesses has unique characteristics, the adversary models must be customized for each project. Sandia's adversary models allow for that.

The Red Team's choice of adversary models is driven by three factors:

- The threats and nightmare consequences identified by the Red Team and customer: More complex nightmare consequences often, but not always, require more sophisticated adversaries.
- The maturity of the system: More mature systems can benefit from Red Team emulation of more sophisticated adversaries, as lower level threats have often already been addressed. Less mature systems profit more from less sophisticated adversarial attack. Since even trivial attacks are likely to succeed, there is little reason to show that high-level attacks are successful.
- Project budget and schedule and information available to the Red Team: Highly sophisticated attacks such as those at the nation state level (Cyber terrorist organizations, Military Information Operations units, and Foreign Intelligence Services) usually require in-depth knowledge of the target system. The Red Team can acquire such information in two ways: synthesize it, limited by project budget and schedule, or obtain it from the customer or system vendor. If these options are limited or not available, the Red Team will not be able to adequately emulate the higher threat levels and will choose to hold adversary capabilities to a lower limit.

DOL Adversary Model

As noted previously in the scope section, DOL management perceived that a potential threat exists from individuals or organizations wishing to profit from premature, unauthorized access to key economic data. Advance knowledge of such data would give its possessor a "head start" advantage against other financial traders who transmitted the information later, during the official release.

According to DOL officials interviewed during this assessment, concern exists over which "press" organizations are allowed access to informational release events. At the heart of the debate is what criteria should define a press organization vs. a business primarily interested in supplying data for algorithmic trading. The line between such entities is blurred by organizations which provide both traditional journalistic content as well as algorithmic trading products to their customers. Interviews with DOL officials indicate this issue is relevant because organizations primarily concerned with algorithmic trading would have significant monetary incentive to circumvent the embargo imposed on key economic data prior to its official release. A New York Times article posted contemporaneously with the writing of this report stated that High Frequency Traders (a type of algorithmic trader) made $12.9 billion in profits in the last two years.[2]

With the assessment scope limited to the press lockup facility and associated data embargo and release processes, the SNL IDART Red Team focused only on adversaries with opportunity, motivation and willingness to subvert security controls specifically associated with this facility. This was an important limitation in that it effectively excluded common adversaries using the Internet as a preferred attack vector[3,4] while DOL Internet connected systems - where the key economic data of interest is produced and stored- are not within the defined scope of CleanSweep. The full spectrum of adversaries is illustrated in Table 1, the Generic Threat Matrix.

		THREAT PROFILE						
		COMMITMENT			RESOURCES			
						KNOWLEDGE		
	THREAT LEVEL	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
High	1	H	H	Years to Decades	Hundreds	H	H	H
	2	H	H	Years to Decades	Tens of Tens	M	H	M
	3	H	H	Months to Years	Tens of Tens	H	M	M
Mid	4	M	H	Weeks to Months	Tens	H	M	M
	5	H	M	Weeks to Months	Tens	M	M	M
	6	M	M	Weeks to Months	Ones	M	M	L
Low	7	M	M	Months to Years	Tens	L	L	L
	8	L	L	Days to Weeks	Ones	L	L	L

Table 1: Generic Threat Matrix. Foregoing potentially loaded terms such as "hacker" or "nation state actor", the Generic Threat Matrix provides a qualitative categorization of adversaries based upon attributes describing their capabilities in terms of technical and organizational capacity.

This matrix provides qualitative values to key adversary attributes, enabling the Red Team to gauge the capability level and attack tools, tactics, and processes such an adversary would bring to bear[5].

Information provided by DOL officials and personnel and gleaned by the SNL team during their assessment activities indicates the following adversary threat profile for the press lockup facility and data embargo and release process:

Intensity: Medium- The threat is moderately determined to pursue its goal and is willing to accept some negative consequences resulting from that pursuit. Acceptable consequences may include imprisonment, but usually not the death of group members or innocent bystanders.

Stealth: Medium- The threat is moderately capable of maintaining a necessary level of secrecy in pursuit of its goal, but is not able to completely obscure details about the threat organization or its internal operations.

Time: Weeks to Months- The threat is capable of dedicating several months to planning, developing, and deploying methods to reach an objective.

Technical Personnel: Tens- The threat is capable of dedicating a small, independent group of individuals to provide the technical capability of building and deploying weapons. There is full communication between the members of the group.

Cyber Knowledge: High- The threat is capable of using expert proficiency- both theoretical and practical- in pursuit of its goal. The threat is able to participate in information sharing and is capable of maintaining a training program, as well as a research and development program.

Access: Medium- The threat is able to plan and place a group member with indirect or limited access within a restricted system.

The **Kinetic Knowledge** category was not used in this analysis, as such capability was not judged to be necessary to compromise the target environment.

The sum of these attributes fall between levels five (5) and six (6), both within the "medium" range of threat actor. The team assessed the adversary here lacked the "high" level of intensity because it is unlikely they would employ violent means to meet their goal of exfiltrating embargoed data prior to the official release time. This adversary has a "high" rating for cyber knowledge capability because of the highly technical nature of algorithmic trading.

In summary, likely adversaries in this scenario are profit-driven, technically sophisticated individuals who may have considerable resources at their disposal. Their technical proficiency enables implementation of stealthy surveillance equipment. Though they are willing to bend and potentially violate rules and laws, there are limits to what these adversaries are willing to do to achieve their goals- violence is unlikely as an operational method.

Analysis

In this section we discuss the attacks that were developed and run by Red Team personnel. Using the IDART methodology, the Red Team begins analysis of the target system and creates the various viewpoints discussed above in the **Error! Reference source not found.** section. Next, the team holds a brainstorming session, inviting Sandia employees that have expertise in the areas addressed by the target system. The Red Team lead describes the target system, presents and explains the viewpoints, and answers any questions before beginning the brainstorming.

During brainstorming, very little filtering is applied to submitted ideas. If an attack idea will obviously not work or violates the ROE, it may be filtered immediately. Otherwise, all ideas are added to the attack graphs and will be filtered later. This allows all ideas to inspire other ideas that may not be filtered.

The result of the brainstorming session is the project's attack graph—a diagram that suggests start states, end states, and attack paths connecting the two states. Many of the attack steps will be invalidated, and some will be filtered because they are beyond

the capabilities of the adversary that we are modeling. The attack graph will remain in constant flux throughout the rest of the project as new ideas are added based on results from testing.

During attack graph development, it often becomes obvious that many attack steps lead to the same nodes. These nodes represent intermediate goals and become the basis for the Red Team's critical success factors.

Attack Graph

Figure 13 shows the DOL press lockup facility attack graph. As noted, scope is limited to External Attackers (non-DOL personnel) attempting to surreptitiously exfiltrate embargoed data from the press lockup facility prior to the official release time. Items on the right of the diagram are preparatory steps or actions [redacted]

Figure 13: DOL Press lockup facility initial Attack Diagram. During this stage, all but the most implausible ideas are captured and discussed. Colors indicate groups of similar or related attacks. Blue vertical bars separate attack stages, starting with preparation (right), execution (center), and goal achievement (left).

Attack steps in the center section of Figure 13 take place during the embargo period, in most cases from within the press lockup facility. Some are follow-on actions to preparatory steps [redacted], while other attacks may be executed without preliminary action [redacted]. The left side of Figure 13 shows any remaining attack steps required to achieve the adversary's goal of premature data exfiltration [redacted]

Post-brainstorming analysis indicated the most plausible attacks fell into three main categories: [redacted], as illustrated in Figure 14.

Figure 14: Consolidated Attack Diagram. Analysis indicated that the most plausible attacks fell into three main categories: [redacted].

Attacks are rated in severity from “critical”, denoting a near-certain likelihood of occurrence, to “low”, denoting an unlikely event. Table 2, Attack Step Risk Ranking System, captures these metrics. None of the attack steps were identified as critical or important.

Rating	Definition
Critical	An attack step that has a near-certain risk of occurring in the future if it has not already happened
Important	An attack step that is very likely to occur in the future and may already have taken place
Moderate	An attack step that is likely to occur in the future and could already have taken place
Low	An attack step that is unlikely to occur in the future and probably has not yet occurred

Table 2: Attack Step Risk Ranking System. For each attack step we provide a statement of what was or could be done by an attacker.

[redacted] **Attacks –** [redacted]

[redacted]

Mitigation Options:

- Modify existing policy to require personal items be kept in lockers ***outside*** of the press lockup room. Divestment should be a prerequisite for room entry. Cost: Low.
- Metal detector at press lockup facility entry. Security checkpoints at building entrances are some distance away from the Lockup facility, and press personnel are not escorted between points. Cost: Medium.
- Remodel press lockup facility with RF shielding. Attenuating material blocks RF communications into or out of the facility. Cost: Medium/High
- Replace computers and other IT equipment in the press lockup facility with DOL owned equipment and remove the private data lines currently in use. Cost: High.
- Retain status quo. Cost: Nil.

[redacted] **Attacks -** [redacted]

[redacted]

Mitigation Options

- Replace computers and other IT equipment in the press lockup facility with DOL owned equipment and remove the private data lines currently in use. Cost: High.
- Prohibit anyone other than DOL personnel or contractors working for DOL from entering communications closets without a technically knowledgeable escort. Cost: Medium.
- Provide/train technically knowledgeable escorts. Cost: Medium.
- Retain status quo. Cost: Nil.

[redacted]

Mitigation Options

- Limit the number of Black Boxes each press organization may use. Cost: Nil.
- Mount Black Boxes to wall or on raised shelves so that the equipment is within plain view. Use uniform, color-coded, DOL-issued cables between Black Boxes and IT equipment. Cost: Low/Medium.
- Adopt tamper evident decals for inventory tags. Cost: Low.
- Replace computers and other IT equipment in the press lockup facility with DOL owned equipment and remove the private data lines currently in use. This would eliminate the need for the Black Boxes altogether. Cost: High.
- Retain status quo. Cost: Nil.

Summary

Though DOL, BLS, and OPA personnel are doing due diligence in their efforts to monitor and control the press lockup facility, SNL IDART observations indicate opportunities for security improvements, ranging from relatively low-cost changes to existing policy up to investing in new IT infrastructure for the press lockup facility. Table 2 Comparison of Mitigation Alternatives, captures the criteria such as cost, risk, and performance for each option. Also included are scheduling requirements relative to SNL follow up activities to verify/validate effectiveness of implementation.

Policy Issues

The data embargo and release process is well established, and enjoys an advanced level of maturity. Requisite data security policies already exist, but may lack optimal implementation.

- Current policy requires press personnel to surrender cell phones in the press lockup facility prior to the distribution of embargoed data. An improvement to this prudent rule would be to collect cell phones and other personal items such as purses, briefcases, tote bags, etc. prior to granting entry to the facility, and securely storing these items outside for the duration of the press release event.
    1. Cost: Low. Approximately $2,200.00 for hardware and shipping plus labor to install.
    2. Risk: Low. Potential pushback from press; potential liability for lost/damaged personal items.
    3. Performance: Medium value. [redacted]
    4. Schedule priority: Medium. Follow-up would consist of observing new process in action.
- Another policy requires that non-DOL personnel be escorted while accessing wiring closets and communications hubs. Ensuring that only technically knowledgeable personnel are given escorting duties would be a significant enhancement to this practice, as would be documenting process and procedures, and training assigned escorts in security concepts (e.g. maintain visual contact on charges for the duration of each visit, limiting the number of visitors per escort, who to contact and what to do should an incident occur, what constitutes an incident).
    1. Cost: Medium. Personnel wages associated with assigning technical staff (vs. non-technical, who potentially have lower hourly cost) and development, documentation, and implementation of training.
    2. Risk: Medium. Pushback from DOL employees regarding additional assignments; lack of qualified personnel; prioritizing current assignments vs. escorting; cost of hiring new staff.
    3. Performance: High. [redacted]

4. Schedule priority: High. Multi-step solution requires early start; potential delays for contract negotiation pertaining to escort duties; policy and procedure development, documentation and implementation of training.

- Press organizations are currently allowed to use their own equipment in the press lockup facility, with some parties implementing complex configurations to include infrastructure-grade networking appliances and utilizing multiple, DOL-supplied Black Boxes. The resulting clutter, power consumption, heat generation, and government expense for supplying Black Boxes could be reduced by changing existing policy to limit each press work area to a standard equipment configuration (e.g. a single computer, monitor, keyboard & mouse).
    1. Cost: None.
    2. Risk: Medium. Pushback from press organizations.
    3. Performance: Medium. Reduces clutter, making Black Box status identification easier; reduces heat generation, power consumption.
    4. Schedule priority: Medium. Though minimal in implementation effort, SNL project period performance (PoP) end is March 2012.
- Another policy option is to completely disallow non-DOL equipment. Cost, risk, performance and technical ramifications of this path are discussed in the next section.

Technical Issues

The presence of non-DOL IT equipment and communications lines in this facility is of concern to the Red Team. The opaque nature of this equipment to DOL, BLS, and OPA stakeholders is a major impediment to ensuring that embargoed data is not released prior to authorization, and the presence of outsider equipment opens attack vectors into the DOL environment. Because DOL may not conduct technical inspection of this equipment or monitor data traffic for unauthorized activity, there is no way to ascertain with certainty that DOL data is not being exfiltrated without DOL authorization.

- Allowing press organization-owned equipment and communication lines in the press lockup facility creates a need for non-DOL maintenance personnel to access DOL communications and data infrastructure. Replacing press-owned equipment and data lines with a DOL-owned solution would remove opportunities for adversaries to compromise critical DOL communications and data infrastructure.
    1. Implementing a DOL-owned IT solution for the press lockup facility would entail the purchasing, configuring, and maintaining such equipment.
    2. An appropriate solution could be tailored to a “bare-bones” configuration to save cost and reduce attack surface. Services limited to Internet access should provide adequate functionality for traditional journalists, while redirecting the burden of enhanced capability away from DOL and onto those who desire it. Applications (e.g. MS Word,

algorithmic trading applications, etc.) would reside on press organization servers, and not be the responsibility of DOL to license, maintain, and patch.

3. Such a solution would likely reduce heat generation and energy costs for the press lockup facility.
4. DOL would have complete control over press lockup facility hardware and software and the ability to monitor as well as terminate/enable data communications.
5. Such a solution would be segregated from DOL Enterprise environments.
    - Cost: High. Approximately $66K for hardware and software, $3.2K annually for licenses, and between 0.5 – 1.0 FTE for maintenance/administration (please see Attachment 2: Cost Estimates for details).
    - Risk: High. Pushback from press; future increases to licensing costs; onus of defending new environment; ensuring segregation from DOL enterprise environment.
    - Performance: High. Eliminates uncertainties surrounding non-DOL equipment capabilities and access to wiring closets; reduces clutter, heat generation, power consumption; eliminates Black Box costs.
    - Schedule priority: High. Complex, multi-phase option requires immediate start to facilitate completion prior to end of SNL PoP.

- [redacted]

    1. Cost: High. Approximately $40K.
    2. Risk: Medium. As with any technical project, unintentional service disruptions may occur, with associated costs to productivity and equipment replacement; in the event that unauthorized surveillance devices are identified, law enforcement must be notified immediately.
    3. Performance: High. Would provide DOL leadership with clean bill of health for their communications infrastructure (up to that point in time).
    4. Schedule priority: Medium. Should ***only*** be done after removing press-owned IT equipment and communication lines ***and*** implementing qualified/trained escorts.

- The Black Box devices currently employed to control the release of embargoed data in the press lockup facility are simple and fairly robust. However, the current concept of operations governing their use makes compromising or circumventing this control mechanism a plausible occurrence. The cluttered nature of the facility, plethora of non-DOL equipment, and multiple instances of Black Boxes for some press organizations, creates opportunities to mask activities designed to neutralize these control devices.

1. Seal Black Boxes with tamper resistant/indicating inventory labels. Develop and implement policy to monitor labels for tampering.
    - Cost: Low. From $9.00/250 basic seals or $1,200.00/20K for hologram seals; personnel time/wages for developing, documenting, and implementing process; auditing/checking for tamper indications.
    - Risk: Low/Medium. [redacted]
    - Performance: Low for basic seals/Medium for hologram seals. [redacted]
    - Schedule priority: Low.
2. Mount Black Boxes to wall or on raised shelves so that the equipment is within plain view. Use uniform, color-coded, DOL-issued cables between Black Boxes and IT equipment.
    - Cost: Low/Medium. Labor for installation; standardized cabling.
    - Risk: Low.
    - Performance: Medium. [redacted]
    - Schedule priority: Medium.

- As noted previously, surreptitious use of transmitting devices was identified as a potential vulnerability. Installing RF shielding in the press lockup facility would mitigate against this vector by attenuating RF signal strength. Products such as foil-backed sheetrock are a relatively inexpensive implementation.
    1. Cost: Medium. Materials + labor.
    2. Risk: Low.
    3. Performance: High. Correctly implemented shielding would greatly reduce the effectiveness of transmitter attacks from within the press lockup facility; this option would eliminate the need for in-room RF monitoring.
    4. Schedule priority: High.

Mitigation	Cost	Risk	Performance	Schedule priority
Replace press-owned IT with DOL IT	**H**	**H**	**H**	**H**
Knowledgeable, trained escorts	**M**	**M**	**H**	**H**
Limit press-owned IT equipment	**None**	**M**	**M**	**M**
Collect and store personal items	**L**	**L**	**M**	**M**
Surveillance Assessment	H	M	H	M
Tamper-evident Seals	L	L/M	L/M	L
Wall-mount Black Boxes	L/M	L	M	M
Install RF Shielding	M	L	H	H

Table 2. Comparison of Mitigation Alternatives. Side-by-side evaluation of relative strengths and weaknesses associated with each security enhancement option. Mitigation alternatives shown in bold with underlining indicate those recommended by SNL IDART personnel who worked on this assessment.

Mitigation Attributes

While the meaning of the **Cost** attribute is intuitively obvious, others may require more explanation.

Risk refers to potentially negative consequences which may occur either directly or indirectly due to a particular mitigation choice.

Performance refers to the extent that a given mitigation option addresses a stated security concern. Generally, the Performance attribute should be greater than or equivalent to the Risk attribute to be considered worthwhile.

Schedule Priority refers to the relative urgency with which a choice must be planned and executed given time limitations imposed by the current Period of Performance for CleanSweep, which ends March 28, 2012.

Observations

ROE Constraints of Note

The SNL IDART Red Team was limited to observation and assessment activities- no active exploitation exercises were performed during the course of CleanSweep. The scope of allowed activities was limited to the press lockup Room and associated data embargo and release processes.

1. Other areas associated with preparation of the target data were not subject to observation and assessment.
2. Operational IT systems associated with preparing/producing the target data were not subject to observation and assessment.
3. Adversary modeling specifically excluded DOL personnel insider threat.

Potential Avenues

The following activities were proposed to DOL but not sanctioned during this activity[1].

1. Technical evaluation and assessment of BLS IT environments.
2. Technical evaluation and assessment of RF environment at BLS.

Recommendations

There are areas for improvement in policy development and implementation, and for technical mitigation strategies to better secure the Press Lockup facility.

Should DOL decide to pursue mitigation options specific to the Press Lockup facility, the Red Team suggests the following measures take priority status:

1. Disallow non-DOL-owned IT equipment and communication lines from the Press Lockup facility or anywhere else on DOL premises.
2. Require technically cognizant escorts accompany non-DOL personnel into wiring closets and communications hubs.
3. Require non-DOL personnel to surrender personal items prior to entering the Press Lockup facility. External storage lockers could secure belongings for the duration of press events.

[1] Current reporting from open and sensitive sources indicates computer targeted network exploitation (CNE) as the most prevalent method of unauthorized data exfiltration from a wide range of adversaries. It is the opinion of Red Team Cyber Security subject matter experts that the IT environments where the data are produced are more likely avenues for data loss than is the Press Lockup facility. CNE offers advantages such as anonymity to an adversary due to the difficulty of conclusively attributing malicious actions over the Internet to specific individuals vs. actions carried out in person in the Press Lockup facility. Compromise of IT systems provides an adversary long-term, unauthorized accesses to potentially valuable information with little chance of discovery.[1]

Attachment 1: Agenda

Project CleanSweep Site Assessment

Han Lin, Project Manager; Scott Maruoka, Technical Lead; Will Atkins, Michael Freund, Lyle Hansen, Technical Team.

7-8 July, 2011

U.S. Department of Labor
Frances Perkins Building – 200 Constitution Ave, NW

Thursday, July 7, 2011

8:30 am	Introductions	All **S-2203 Conference Room**
9:00 am	DOL/BLS Mission & Goals	Ed Hugler *Deputy Assistant Secretary for Operations* Carl Fillichio *Senior Advisor for Communications and Public Affairs* Michael Levi *Associate Commissioner, BLS Office of Publications and Special Studies* **S-2203 Conference Room**
9:30 am	SNL IDART Agenda	Han Lin, Michael Freund, Lyle Hansen *Manager, Networked Systems Survey & Assurance; Technical Team* **S-2203 Conference Room**
10:00 am	Introduction to IDART	Will Atkins & Scott Maruoka *IDART Team*
11:00 am	Break	**S-2203 Conference Room**
11:15 am	Introduction to IDART	Will Atkins & Scott Maruoka *IDART Team*
12:00 pm	Lunch	**S-2203 Conference Room**
1:00 pm	Technical Team setup.	Michael Freund, Lyle Hansen
1:00 pm	Facility Wireless System Assessment	Will Atkins
1:00 pm	Interview with Jermaine Pegues.	Han Lin, Scott Maruoka **S-2203 Office**
1:30 pm	Interview with Gary Steinberg.	Han Lin, Scott Maruoka **S-2203 Office**

2:00 pm	Interview with Rick Vaughn.	Han Lin, Scott Maruoka S-2203 Office
2:30 pm	Interview with Anthony Ferreira.	Han Lin, Scott Maruoka S-2203 Office
3:00 pm	Interviews with Carl Fillichio.	Han Lin, Scott Maruoka S-2203 Office
4:00 pm	SNL Team Members depart	All

Friday, July 8, 2011

6:30 am	Briefing Preparation	SNL Technical Team
8:00 am	Press Briefing	SNL Technical Team
9:00 am	Interview with Jennifer Kaplan	Han Lin, Scott Maruoka N-1649 Conference Room
9:30 am	SNL Team Discussion & Analysis	SNL Technical Team N-1649 Conference Room
12:00 pm	Lunch	
1:00 pm	Presentation of Initial Findings	SNL Technical Team N-1649 Conference Room
3:00 pm	SNL Team Members depart	All

Attachment 2: Cost Estimates

The following information represents rough cost estimates for selected mitigation options documented in the main body of this report. It should be noted that costs are subject to changes not within SNL IDART control, such as vendor adjustments and local conditions (e.g. union rates, local & state taxes and fees).

DOL-owned IT solution

SNL computer network infrastructure subject matter experts provided the following information for a potential diskless solution to replace the current press-owned IT equipment deployed in the Frances Perkins Building press lockup facility.

A thirty (30) seat diskless architecture consisting of Wyse clients and VMware backend (VSphere and VMware View), server hardware, and associate licenses would cost approximately $66,000 to purchase software and hardware. Licenses would cost approximately $3200 annually. This estimate excludes operating system licensing costs. MS Windows (or other OS) licenses could be added to current contracts. Implementation and maintenance of the system is estimated at one (1) full time employee (FTE) and 0.5 FTE respectively.

Component	Purchase	Licensing
Servers	$25K	
VMware components (vSphere + View)	$26K	$3.2K/year
Wyse clients (x30)	$15K	
Total	**$66K**	**$3.2K/year**

Table 1. Estimated acquisition and licensing costs for a diskless IT infrastructure.

Surveillance Assessment

Approximately $40K, based on SNL Financial Analyst projections for two (2) technical subject matter experts conducting an assessment of two (2) weeks duration.

Shielding

TBA

Lockers

Three vendors were identified via Google search, with the following cost results for hardware and delivery. All estimates are for Eight wall-mounted, four-locker units.

Bigdoglockers.com: http://www.bigdoglockers.com/
Penco Vanguard Quickship Metal Wall Mount Box Locker
Product ID: 68242X
Weight : 43.00 lbs
Legs : Legs

Vanguard Metal QS Assembly : Assembled
Vanguard Metal QS Color : Grey
Cost: $1,279.92; shipping: $880.00; Total: $2,159.92

Lockers and Storage Catalog: http://lockerscatalog.com/items.asp?Cc=LLOCK-QSW&iTpStatus=0
Hallowell® Wall Mounted Premium Box Locker
Product ID: L236-1095
Weight: 50 LB
Dimensions: 48” W X 18” D X 12” H
Color: Grey
Unassembled
Cost: $1,440.00; shipping: $880; Total: $2,320.00

Lockers.com: http://www.lockersupply.com/
Penco Quick Ship: Vanguard Unit Packaged Lockers - Four-Wide Wall Mount - 68242
SKU #: PN1122
Dimensions: 13.625" H x 45" W x 18" D 43.0 lbs.
Unassembled
Cost: $1,463.92; shipping: 116.19; Total: $1,580.11

Tamper-evident Labels

Tamperco: http://www.tamperco.com/Tamper_Void_Tamper_Evident_Labels_s/22.htm
Tampervoid labels: $9.00/250
Hologram labels: $1,200.00/20K

References

[1] Eugene Register-Guard (no author attributed),Labor building named for 'Madame Secretary', April 11, 1980, http://news.google.com/newspapers?id=jlMRAAAAIBAJ&sjid=3eEDAAAAIBAJ&pg=5679,2910817&dq=frances-perkins-building&hl=en

[2] New York Times (no author attributed), High Frequency Trading, August 9, 2011, http://topics.nytimes.com/topics/reference/timestopics/subjects/h/high_frequency_algorithmic_trading/index.html?scp=1-spot&sq=High%20Frequency%20Trading&st=cse

[3] Cisco, Cisco 2010 Annual Security Report, http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf

[4] Alperovitch, D. Revealed: Operation Shady Rat, McAfee Blog Central, http://home.mcafee.com/AdviceCenter/ExternalContent.aspx?id=cm_malb

[5] Dugan et al, Sandia National Laboratories, Categorizing Threat: Building and Using a Generic Threat Matrix, September 2007.