SANDIA REPORT
SAND2011-xxxx

Printed August 2011

CleanSweep Red Team Report

Prepared for:

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
Red Team Project Lead
Sandia National Laboratories
P.O. Box 5800 MS 0620
Albuquerque, NM 87185-0620

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 Lin
Project Manager
(505) [redacted]
[redacted]@sandia.gov

Table of Contents

Executive Summary

Over the course of the last four years, the Department of Labor (DOL) was approached by various regulatory authorities 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 media reporters and the general public. The objective for CleanSweep was to identify potential vulnerabilities in the DOL press lockup 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 has its own unique perspective regarding the nature of the perceived threat and, consequently, differing ideas on potential solutions. The common concern amongst these stakeholders revolves around the unauthorized, premature release of embargoed data.

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

Although 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 are 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 employees and contractors working for these press organizations to conduct maintenance. This access, though controlled by DOL personnel escorting such outsiders, creates opportunities for adversaries to compromise critical DOL communications and data infrastructure.

The following actions could 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.
- 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 facility. Divestment should be a prerequisite for entry.

Although not directly addressed in the Sandia National Laboratories (SNL) Red Team analysis, the apparent root cause for the issues driving this assessment is the possible presence of algorithmic traders and/or their agents in the press lockup facility. Modifying DOL policy on what criteria qualifies applicants to attend release events would likely be of benefit.

How to Use This Report

This report documents Sandia National Laboratories' (Sandia's) Information Design Assurance Red Team (IDART) security analysis of the United States Department of Labor (DOL) press lockup facility. The first section, the Management Overview, is intended for members of DOL management and provides an overview of the activity without technical details. Readers interested in knowing at a high level the threats to DOL information systems, and how to protect against those threats, should examine the Attack Diagram Description presented in the results section of the Management Overview. Readers who want to know how the Red Team conducted its assessment should read the Management Overview in its entirety.

It is worthy to note that because Sandia's analysis revealed verified vulnerabilities in processes, procedures, and systems used to protect DOL-embargoed data, the public version of Sandia's report to DOL (this document) is intentionally kept at a general level. Representatives from DOL have encouraged the release of this summary to the public.

Management Overview

The analysis described in this report—designated project CleanSweep—was conducted at the request of the United States Department of Labor (DOL). This section is organized around the simplified attack diagram (Figure 2. Press lockup Facility Attack Diagram) developed by the Red Team, describing the most plausible attacks against data confidentiality in the press lockup facility. The descriptions of steps in each attack provide a high-level view of the attack, an impact estimate for a successful attack , and the recommended mitigations to prevent that attack step. The following sections provide background for the attack diagram.

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 media reporters and the general public. The focus of DOL management concern is the physical, technical, and procedural controls which constitute this embargo process.

Objective

The primary objectives of CleanSweep were to identify potential vulnerabilities in DOL press lockup 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.

Sandia's IDART team executed the following assessment activities:

1) Analysis of available security processes, procedures, rules, security equipment technical specifications, floor plans, and other artifacts relating to the press lockup facility and embargo process.
2) 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 (ROE) for assessment activities.
3) 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 press lockup facility, associated communications infrastructure, and technical security equipment. IDART team members also conducted interviews with DOL personnel tasked with implementing and executing the embargo process.
4) SNL technical specialists executed exterior and interior surveys of the radio frequency (RF) spectrum in the area of interest, and conducted another RF spectrum analysis during an information embargo/release event.

Findings from these assessment activities were analyzed using the IDART methodology described throughout this document, and a subset of 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. DOL agreed to provide access and support to SNL IDART team members during assessment activities. The ROE were developed by SNL IDART personnel in concert with DOL officials, and were formulated to ensure that 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. Each press agency with access to the facility owns and maintains its own equipment, including the communications lines to the outside world. The IDART 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 the July 8, 2011 press release.

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 security posture for the target environment. In reality, project budget and schedule always 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 DOL, the DOL 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 IDART 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.
- RF environment for the area of interest.
- Computer and communications equipment in the press lockup facility.
- Communications infrastructure for the press lockup facility.

The IDART team specifically did not consider the following:

- Threats and vulnerabilities associated with persons possibly acting as “insiders” at DOL.

- Threats and vulnerabilities associated with DOL IT systems used in the acquisition of data and production of finished economic analysis.
- Surveillance vulnerabilities at locations other than the press lockup facility but associated with the data embargo and release process.
- The parallel television media embargo/release facility and its associated processes.

Red Team Composition

Sandia/IDART created a team whose members possess skills specifically applicable to addressing the various issues presented by this project. The team consisted of five (5) members with technical specialties including cyber security and threat assessment, adversary modeling, physical security design and threat assessment, electronic surveillance, and risk management.

Analysis Environment

The IDART team conducted preliminary analysis of information acquired during its assessment while at DOL, which was communicated to DOL stakeholders during an out-briefing at the conclusion of assessment activities. Upon returning to the Sandia, the IDART team and an IDART subject matter expert (who did not accompany the team to DOL) conducted further analysis to identify and then refine potential attack scenarios and appropriate mitigation strategies.

Methodology

For Project CleanSweep, the IDART team used a subset of the IDART methodology illustrated in Figure 1. This 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 to the budgetary and scheduling realities of a project. We accept that complete understanding of a highly complex system or environment is impractical for most projects, and we use the IDART process to generate meaningful assumptions and realistic, simplified representations for the target environment. 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/environment affects the applicability of the IDART process. Targets must have a reasonable level of maturity—be it in the operational or design phase—in order to support an IDART methodology assessment.

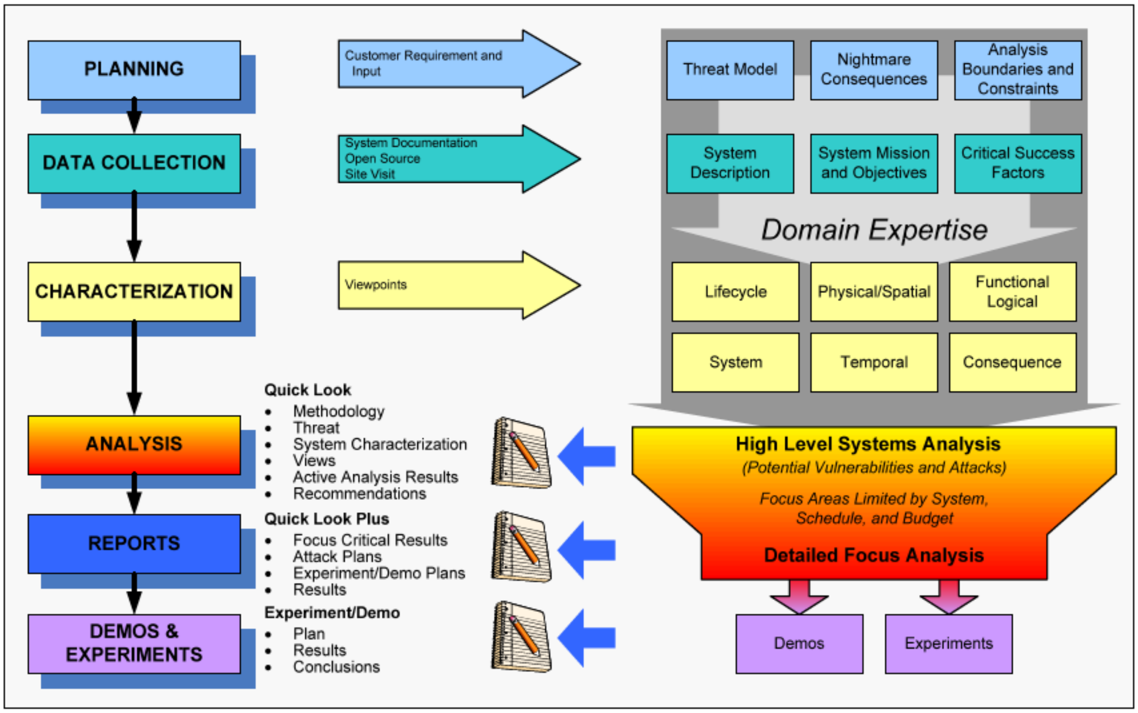


Figure 1: IDART Methodology. The IDART team lead first negotiates with the customer requirements, rules of engagement, threat models, nightmare consequences, and other administrative items. Assessment activities begin with collecting data on the target system/environment, then viewpoints are developed from the data that highlight target system dependencies, critical success factors, and other characteristics. These viewpoints feed the red team analysis, where vulnerabilities are discovered and chained together to form attacks that result in the adversary achieving their goal (the customer's "nightmare consequences").

In the next few sections we describe the initial products of the planning phase—Threat Model, Nightmare Consequences, and Boundaries and Constraints.

Threat Model

The IDART methodology begins by developing a threat model to guide and inform 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, motivations, and levels of commitment. Establishing an adversary model allows analysts to postulate more accurately on what types of attack tools, techniques, and procedures will likely be brought to bear against defenders, and so instruct as to the most appropriate mitigation strategies to employ.

DOL Adversary Models

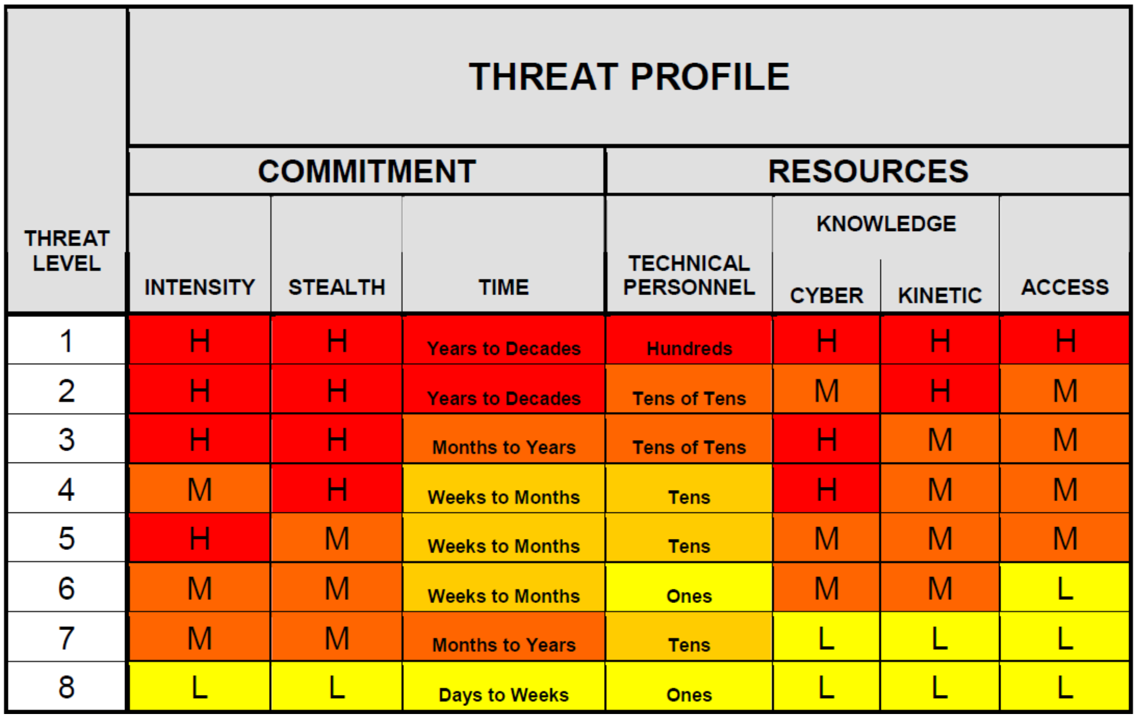
As noted previously in the Scope section, DOL management perceived that a potential threat existed from individuals or organizations wishing to profit from premature, unauthorized access to key economic data. Advance knowledge of such data could give its possessor a “head start” advantage against others who received the information following the official release.

According to DOL officials interviewed during this assessment, concern exists over “press” organizations allowed access to informational release events. At the heart of the issue is what criteria should define a press organization versus 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. According to DOL officials, this issue is relevant in that organizations primarily concerned with algorithmic trading would have significant monetary incentive to circumvent the embargo imposed on key economic data and act on it 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[i]. Of particular challenge to DOL is the reality that algorithmic traders can successfully profit from possession of embargoed data only fractions of a second prior to its official release.

With the assessment scope limited to the press lockup facility and associated data embargo and release processes, the IDART team focused only on adversaries with opportunity 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[ii,iii] while DOL Internet connected systems—where the key economic data of interest is produced and stored—are not within the defined scope of CleanSweep[1]. The full spectrum of adversaries is illustrated in Table 1, the Generic Threat Matrix[iv].

[1] The IDART team recommends examination of BLS IT systems used to produce the target economic data, and review of personnel security controls to address potential compromise of insiders. While not within the scope of CleanSweep, these are the most likely vectors for data leakage.

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.



THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
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
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
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

This matrix provides qualitative values to key adversary attributes, enabling the red team to gauge the capability level and attack tools, techniques, and procedures (TTPs) such an adversary would bring to bear.

Information provided by DOL officials and personnel and gleaned by the IDART 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 TTPs. 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) in the Generic Threat Matrix (Table 1), 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 or organizations who may have considerable resources at their disposal. Their technical proficiency enables implementation of stealthy surveillance equipment. Although they are willing to bend and potentially violate rules and laws, violence is unlikely as an operational method.

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 achieve them within the limitations of the identified adversary's capabilities. Since CleanSweep activities were limited to assessment and observation, red team activities 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—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
- Accountability in potential widespread financial implications

Boundaries and Constraints

All simulated attack scenarios were limited to data exfiltration attacks from within the press lockup facility; potential adversaries were limited to non-DOL personnel.

Results

The attack scenarios most likely to succeed fit into three main categories: hidden transmitters, compromised communications infrastructure, and subversion/circumvention of DOL technical countermeasures ("Black Boxes," devices DOL has in place to turn on/off press-owned communications terminating in the press lockup facility). All of these potential attacks would have a high likelihood of success under current conditions.

Attack Diagram Description

The attack diagram is shown in Figure 2. The diagram shows the various high-level attack paths an adversary might use to achieve the nightmare consequences. The adversary is assumed to be an external attacker (non-insider) for all the attacks considered in this assessment (as per the red team constraints and ROE).

[redacted]

Figure 2: Press lockup facility attack diagram. [redacted]

Attacks are rated in severity from “critical”, denoting a near-certain likelihood of occurrence, to “low”, denoting an unlikely event. Figure 2 captures these metrics.

Table 2: Attack step risk rankings. For each attack step we provide a statement of what was or could be done by an attacker.

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

[redacted] Attacks

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Mitigation Options

- Modify existing policy to require personal items be kept in lockers *outside* of the press lockup facility. 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.
- 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.
- Remodel press lockup facility with RF shielding. Attenuating material blocks RF communications into or out of the facility. Cost: Medium
- Retain status quo. Cost: Nil.

[redacted] Attacks

[redacted]

[redacted]

[redacted]

[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: Low
- Provide/train technically knowledgeable escorts. Cost: Low/Medium.
- Retain status quo. Cost: Nil.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[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.

Management Results Summary

The results of IDART's assessment are as follows:

- Although 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. 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.
- DOL communications and data infrastructure access to press organizations' maintenance contractors is an issue. This access, though controlled by DOL personnel escorting such maintenance personnel, creates opportunities for adversaries to compromise critical communications and data infrastructure.
- 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.

As a result of the assessment activity, the IDART team made several recommendations to improve the security of DOL systems. The most important of these recommendations include the following:

- 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 facility. Divestment should be a prerequisite for room entry.

Although not directly addressed in the IDART analysis, the apparent root cause for the issues driving this assessment is the possible presence of algorithmic traders and/or their agents in the press lockup facility. Modifying DOL policy on what criteria qualifies applicants to attend release events would likely be of benefit.

References

[i] New York Times (no author attributed), High Frequency Trading, August 9, 2011

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

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

[iv] Duggan, David P., Thomas, Sherry R., Veitch, Cynthia K. K., Woodard, Laura. “Categorizing Threat: Building and Using a Generic Threat Matrix”. SAND2007-5791. Available: http://energy.gov/oe/downloads/categorizing-threat-building-and-using-generic-threat-matrix

[v] Black Box® Network Services (BBOX). http://www.blackbox.com/