SECURITY AWARENESS PLAN

## Defense Contractor Sheltered Laboratory

# Table of Contents

[Defense Contractor Sheltered Laboratory](#_heading=h.30j0zll) 1

[**Table of Contents**](#_heading=h.44sinio) **2**

[**Readme**](#_heading=h.cfmh54ruh13i) **3**

[**Project Charter**](#_heading=h.1pxezwc) **4**

[**Advisory Board**](#_heading=h.ey3r1nsrgys8) **7**

[**Project Implementation Plan**](#_heading=h.gg37q0158wyt) **9**

[Executive Summary](#_heading=h.147n2zr) 9

[Target Audience (WHO)](#_heading=h.rhswwfezqzqe) 10

[User Group 1 - Algorithm Staff](#_heading=h.23ckvvd) 11

[User Group 2 - Security Staff](#_heading=h.ihv636) 11

[User Group 3 - I&T Staff](#_heading=h.32hioqz) 12

[Operating locations](#_heading=h.1hmsyys) 13

[Risks (WHAT)](#_heading=h.ja6lixg77327) 14

[Risk Prioritization](#_heading=h.ubdqccedqh2h) 14

[Top Risks](#_heading=h.vx1227) 16

[Data Security](#_heading=h.3fwokq0) 16

[Physical Security](#_heading=h.1v1yuxt) 16

[Passwords](#_heading=h.4f1mdlm) 17

[Strategies (HOW)](#_heading=h.6hgmd79zsvpc) 18

[Overall Engagement Strategy](#_heading=h.19c6y18) 18

[Organizational Culture](#_heading=h.3tbugp1) 18

[Formal Training Methods](#_heading=h.28h4qwu) 19

[New Hires](#_heading=h.nmf14n) 20

[Branding and Imagery Decisions](#_heading=h.37m2jsg) 20

[Sustainment](#_heading=h.1mrcu09) 20

[Metrics](#_heading=h.q5ckq0lw8bq6) 21

[Metric 1 - Exposed Devices](#_heading=h.2lwamvv) 21

[Metric 2 - Unlogged Information Transfer/Exposure](#_heading=h.111kx3o) 21

[Metric 3 - Password Issues](#_heading=h.3l18frh) 21

[Appendix A - Learning Objective - Data Security](#_heading=h.wcmqwhxluip3) 22

# Readme

The document below is a security awareness plan based on a common subsection of a Department of Defense (DoD) contract at the Northrop Grumman Corporation (NGC). It is not a security awareness plan for the entire Northrop Grumman organization for two reasons; firstly, it is not feasible to tailor a security plan to meet the diverse requirements of each contract within a multinational company like NGC in anywhere near a reasonable amount of space. Secondly, there is value in evaluating the personnel security awareness requirements for this common subset of engineers who evaluate technical data in a Secure Compartmented Information Facility (SCIF), known internally as the lab. Creating a plan at the program level would have been another valid option, but because of the size and diversity of roles within my current program, it would still be impossible to cover the different requirements in enough detail to be useful within the page limit. The following awareness plan changes the names and details to protect operational security.

Many times, as security architects in the defense contracting industry, we are required to adhere to a wide variety of frameworks and technical compliance checklists; but it is easy to overlook the importance of training the human element for behavior change and effectiveness rather than merely meet internal and external requirements. I am choosing to create a security awareness plan for the lab to focus on a subsection of my organization that I can immediately affect with leadership support. The tailored lab security plan can also leverage resources created by NGC.

The lab is in the United States, and all of the members (roughly 30 at any time) hold an active security clearance and are US citizens. There are up to fifteen computers in the lab, all of which are rated for United States Secret level information, but these computers routinely move between two sites - one NGC and one US Army test site. This movement complicates security efforts for both training and maintaining technical controls. The lab currently has a security plan, but it does not include security awareness training.

# Project Charter

|  |  |
| --- | --- |
| **Sheltered Lab Security Awareness Program – Charter** | |
|
| **Program Title:** | Sheltered Lab Security Awareness Program |
| **Owner:** | The Deputy Program Manager (DPM) is the project sponsor. The Cyber Team will be responsible for building, maintaining, and measuring the security awareness program and will report directly to the DPM. |
| **Estimated Costs:** | $26,000 a year |
| **People Requirements:** | The existing two-person Cyber Team will administer the program as an additional duty. The administration of non-security awareness tasks in the lab already requires 0.25 FTE; the addition of a security awareness program will add 0.25 FTE. |
| **Finalize Plan Date:** | 15 / 12 / 2019 |
| **Program Launch Date:** | 01 / 03 / 2020 |
| **Scope:** | All program employees and contractors with approved lab access. Specifically, members of the Algorithm Team and anyone with lab computer access. Not in scope are facilities managers, external security managers, and others with infrequent access to the lab. |
| **Description** | This security awareness program is a narrowly scoped communications and training effort to manage our human risk in the classified program lab. The awareness program does this by identifying our top human risks, and the behavior changes needed to manage those risks. The Cyber team uses this information to tailor training to all employees and contractors in scope. This tailored training is meant to change risky behaviors and eventually create a security-minded culture. |
| **Goals:** | Deliver a security awareness program that measurably improves the sheltered lab’s overall security posture by identifying, prioritizing, and reducing our human risk. The program will also focus on educating employees and ensuring compliance with Defense Security Service (DSS) and company policy. We are currently somewhere between the "Non-Existent" and "Compliance" stages of the Security Awareness Maturity Model. NGC has a security awareness program, and this program is a supplement to that. Our goal is to achieve “Promoting Awareness and Behavior Change” by Q3 2020, “Long-Term Sustainment and Culture Change” by 2022, and a genuinely mature program, the “Metrics Framework” by 2023. |
| **Objectives:** | 1. Compliance with Northrop Grumman Corporation (NGC), Department of Defense (DoD), and DSS regulations. |
| 2. Ensure that employees and contractors understand and comply with policies, processes, and procedures. |
| 3. Identify the top five human risks to our lab and manage those risks by changing employee/contractor behavior. |
| 4. Identify the top five most confusing/complex policies and procedures that are negatively impacting our workforce and work to simplify those processes or perhaps even eliminate them through other controls. |
| 5. Create and support a human sensor network of employees to reduce the occurrence of security violations and workarounds while also proactively identifying potential problems before they occur. |
| 6. Implement metrics program to track and report on the impact of our program. |
| 7. Build and maintain leadership support long term, to include regular briefings that demonstrate program impact and value. |
| 8. Create a positive, security-aware culture where people feel responsible for physical and information security in the lab. We also aim to produce a cooperative culture between employees in the lab and the Cyber Team. |
| **Justification:** | This security awareness program will reduce the risk of information disclosure and ensure compliance with NGC, DSS, and DoD requirements. This program supplements the existing NGC security awareness program. The priority is to ensure compliance since non-compliance is an existential threat to our program. A failure could lead to loss of the lab or even of the contract. Ensuring compliance creates a baseline of knowledge to build on. Second, the security awareness program will reduce our exposure to various risks that technical controls alone cannot mitigate. In the past 24 months, our program has received authority to operate our classified lab, but we have identified various instances where people have not adhered to either security policy or best practices. These violations of policy can be costly to NGC and the program in both money (needing to pass recertification and investigate information disclosure) and reputation (not being trusted to safeguard sensitive data). A security violation can easily result from relaxed enforcement of access control to the lab (letting someone in), integrity controls (unauthorized software or even malware entering the lab), authentication controls (sharing passwords), or handling of classified information (inadvertent disclosure of sensitive information). Creating a culture of security awareness through a mature security awareness program can reduce the risk of information disclosure and improve the financial and reputation outcomes of both the program and NGC. |
| **Milestones:** | Select and build Security Awareness Advisory Team, include key influencers on program Cyber Team (administers and develops program), Algorithm Team (the majority of lab engineers), NGC ISSM (lab owner), and Deputy Program Manager (key stakeholders). |
| Collaborate with NGC CSOC, ISSM, program Cyber Team, Army security liaison, and lab staff to collect statistics on past security incidents for our lab and similar labs for other programs. |
| Consult with program Cyber Team, NGC ISSM, and lab Security Awareness Advisory Team to identify areas with the largest risk exposure in our lab. Identify security practices that mitigate these risks and associated behavior/procedure changes that need to happen. |
| Create a security awareness plan using prioritized risks and mitigations identified by the Security Awareness Advisory Team. |
| Approval of plan/budget by program leadership, including Deputy Program Manager, Algorithm Staff Team lead, Cybersecurity Team Lead, and Business Advisory Team (Legal and Compliance). |
| Create training materials |
| Begin rollout of monthly lab security training hour and discussion. |
| The Security Team briefs the DPM and ISSM on program events and outcomes. |
| Roll out reinforcement training. |
| Begin assessments, feedback, and reporting. |
|  |
| **Assumptions and Constraints:** | Algorithm team support. |
| Because of the small size of the team and their experience with other information security programs, there should be a rapid path to achieve a mature program. |
| We have access to Company Security Operations Center (CSOC), Information System Security Manager (ISSM), and Army security liaison for historical data. |
| Constraints include: |
| High turnover in lab staff may present training challenges |
| Employees have limited time available for training. |
| Getting all employees together at one time |
| **Critical Success Factors:** | At least 0.25 dedicated Full-Time Employees to run the security awareness program, 0.5 would be ideal |
|  |
| **Go/No-Go** | Approved/Rejected |
| **Comments:** |  |
|

# 

# Project Implementation Plan

## Executive Summary

Northrop Grumman defense contracts have legal requirements to keep sensitive information secure. Effective security measures are also required to meet Northrop Grumman’s core values of responsibility, trust, integrity, and protecting freedom. Our ability to fulfill these obligations can have huge impacts on the program financially, and on Northrop’s trustworthiness as a government contractor. The classified lab processes large amounts of sensitive radar and sensor data. In the last six months, we have implemented many technical controls, such as two-factor authentication tokens (2FA), automated security log collection, SIEM, and access checks. These controls help us meet the requirements of DoD, DSS, and NGC regulations we must follow, but there is no security awareness plan to address the critical human elements specific to the lab. While Northrop Grumman has mandated annual security awareness training, it is often broad in scope and does not address specific areas of concern for the lab. This plan is an excellent supplement to the annual NGC training but tailored to our program’s unique needs.

The lab has had numerous security incidents involving the lab or lab staff in the last two years. These incidents have occurred both at the program office and the government test site. Interviews with lab staff have established that these incidents occurred primarily because of complacency and lack of knowledge on proper procedures. One of these had a significant impact on our ability to work at the government test site and caused harm to the reputation of the program. These incidents cannot be allowed to become a trend.

A security awareness program enables us to deliver training and track metrics relevant to the needs of our lab environment. Training includes quarterly lunch seminars with lab members and monthly focus groups with subsections of the lab team. Metrics such as training attendance tracking and security violation tracking will be reported to the program manager quarterly. This program will require an investment of 0.25 FTE, and the current Cyber Team will administer it. This investment will enable us to more effectively meet legal requirements while maintaining our reputation as a government defense contractor focused on delivering ‘The Value of Performance’ as a C4ISR leader. Just as importantly, this program will work to improve the security culture for the lab, reducing security incidents by correcting the attitude of complacency and lack of knowledge about procedures. Creating a culture of security through awareness training is both more cost-effective and responsible than responding to incidents with policy statements or technical controls because it addresses the root of the problem.

## 

## Target Audience (WHO)

We will tailor the security awareness plan for the lab to the primary user groups. Tailoring the training helps to more effectively change security-related behaviors since each group has distinct demographics, risk levels, and engagement strategies. Properly identifying user demographics helps awareness training to be more effective because it matches learning preferences with how information is presented (modality). Different user groups of the lab also have different levels of risk. This risk takes into account the frequency of lab use, frequency of travel with lab resources, the sensitivity of information used in job tasks, level of physical access to the lab (locks, open/close privileges), and level of information system access (normal vs. super users/admins). Higher risk levels will require more tailored training.

The Cyber Team has identified three primary user groups for tailored training. While it would be possible to create even more groups, and this may even moderately improve security outcomes, it is not cost-effective to make too many groups because each group represents a significant investment of time and money. Three groups are the best combination of effectiveness and efficiency. The next page lists the different groups identified in priority order of risk. Please note that two users currently fit into both Algorithm Staff and Security Staff – these users will train with the Algorithm Staff but will receive minutes from the Security Staff meeting.

Training for the different groups will also be rolled out in the order below. Because the Algorithm Staff has the highest frequency of use for the lab, and because they represent the highest aggregate risk, they will receive priority training. The Security Staff group will receive training next; they are ranked second in risk because while they have more privileges in the lab, they generally already have more of a security mindset and use the lab less frequently. The I&T Staff is the lowest priority because of infrequent use paired with lower privileges. We aim to start training a new group every quarter - with the Algorithm Staff starting in Q2 2020, Security Staff in Q3 2020, and I&T Staff in Q4 2020.

### User Group 1 - Algorithm Staff

|  |  |
| --- | --- |
| **ALGORITHM STAFF** | |
| **Description** | The Algorithm Staff analyze radar data and develop better models to track objects. They also develop machine learning models. |
| **Demographic snapshot** | Almost exclusively male over 35 with an advanced engineering degree. Half of the team is over 45. Most of the team is very technically inclined with math/physics but not computer literate outside of Matlab/Microsoft Office. |
| **Requirements** | Most critical group because of routine access to sensitive data  1. Focus on the importance of not working around policy – education about how to get what is needed within the current system.  2. Focus on the dangers of information disclosure.  3. Physical security training needed for travel requirements.  4. Password sharing and reuse dangers - focus on usable solutions. |
| **Frequency of use** | Most Algorithm Team members use the lab daily or every other day for 3-5 hours per visit. |
| **Frequency of travel** | Quarterly travel to the government test site with computers. |
| **Sensitivity of information** | USG Secret level routinely used – specialized technical knowledge is a target of interest for foreign threat actors. |
| **Level of physical access** | Routine daily access. Need Security Team assistance to access lab, safes, computers when at the program office. Have unimpeded access to computers and safes when at the government test site. |
| **Level of IS access** | All members are normal (unprivileged) users. |
| **Total members** | **10** |

### 

### User Group 2 - Security Staff

|  |  |
| --- | --- |
| **SECURITY STAFF** | |
| **Description** | The Security Staff have open/close privileges for the lab. |
| **Demographic snapshot** | Ages vary between 30-55. Most are security or IT professionals with over ten years of DoD or contractor experience. |
| **Requirements** | Second most critical group: more access but less frequent use  1. Focus on the importance of following a physical security procedure.  2. Identify risky signs of behavior/information disclosure.  3. Maintain vigilance on insider threats. |
| **Frequency of use** | Daily. At least one Security Team member will open/close the lab – little to no routine use of information processed in the lab. |
| **Frequency of travel** | Once a year at most. |
| **Sensitivity of information** | Infrequent use of USG Secret level information. |
| **Level of physical access** | Most physical access. All access is logged. |
| **Level of IS access** | Half of the Security Team Staff have administrator/ superuser privileges. |
| **Total members** | **6** |

### 

### User Group 3 - I&T Staff

|  |  |
| --- | --- |
| **INTEGRATION AND TEST STAFF** | |
| **Description** | Integration and Test Team evaluate telemetry and link data from program systems. This data sometimes is from combat operations and is thus marked as USG Secret. |
| **Demographic snapshot** | The integration and test team is younger than the other two groups (most are under 30) with a mix of men and women. The average member has an engineering degree. |
| **Requirements** | 1. Focus primarily on the importance of physical security, including rules regarding prohibited lab items.  2. Identify critical information that needs to be protected. |
| **Frequency of use** | Infrequent use. One member may use the lab for a few hours each week. There is an increased use one week out of the quarter. |
| **Frequency of travel** | Travel with the Algorithm Team, but limited use of the lab systems. |
| **Sensitivity of information** | Sensitive information about operational locations and telemetry data. |
| **Level of physical access** | Infrequent access. Require security staff help to access computers and safes. |
| **Level of IS access** | Normal users |
| **Total members** | **22** |

## 

## 

## Risks (WHAT)

### Risk Prioritization

The security awareness program operates with limited resources of time and money, and the users of the lab have limited time and attention they can spend on training. For these reasons, it is important to prioritize some training requirements over others. We cannot train everything at once. We used risk analysis to look at the probability and impact of any security-related incidents, using these estimates and ratings to determine which training requirements to prioritize. As the training program matures and the top risks are mitigated, the lower-ranked risks will receive more attention.

|  |  |
| --- | --- |
| **PROBABILITY** | |
| Very High | > 95% |
| High | 80%-90% |
| Medium | 20%-80% |
| Low | 5%-20% |
| Very Low | < 5% |
| **Chance of an event happening in the next six months** | |

|  |  |
| --- | --- |
| **IMPACT** | |
| Very High | Loss of life; loss of >$10 million; Permanent reputation damage; Congressional report; shutdown of operations > 5 days |
| High | Critical injury; $1-10 million loss; long-term reputation damage; Management legal consequences: 1-5-day shutdown |
| Medium | Severe injury; $100k - $1 million loss; serious reputational damage; 1-day shutdown |
| Low | Employee Injury; $10k-$100k loss; some reputational damage  minor legal proceedings; <24-hour shutdown |
| Very Low | Minor injury; <$10k loss; minimal reputational damage; < 1-hour shutdown |
| **The human, financial, or reputation cost of an event** | |

Score calculator: X-axis is Impact, Y-axis is Probability

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | VL - 1 | L - 2 | M - 3 | H - 4 | VH - 5 |
| VH - 5 | 5 | 10 | 15 | 20 | 25 |
| H - 4 | 4 | 8 | 12 | 16 | 20 |
| M - 3 | 3 | 6 | 9 | 12 | 15 |
| L - 2 | 2 | 4 | 6 | 8 | 10 |
| VL -1 | 1 | 2 | 3 | 4 | 5 |

\*\*P = Probability, I = Impact, S = Risk Score\*\*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **RISK** | **Description** | **P** | **I** | **S** |
| **Data Security** | Applying proper safeguards, labeling, and classification guides to ensure sensitive information is protected. | 4 | 5 | 20 |
| **Physical Security** | Physical security measures to prevent unauthorized access to information, people, and equipment | 4 | 4 | 16 |
| **Passwords** | Current password requirements and why longer passphrases and 2FA are needed. Dangers of password sharing and other practices that hurt authentication/ non-repudiation. | 5 | 3 | 15 |
| **Targeted attacks** | Identify what targeted attacks look like and how to report them. Understand that people want to know what you know. | 3 | 4 | 12 |
| **Privileged access** | The Security Team has special responsibilities with both physical and information system access to the lab. Explain the scope of responsibility and weak areas. | 2 | 5 | 10 |
| **Mobile Device Security** | The use of mobile devices risks revealing sensitive information. Understand lab and test site rules on personal computing devices, including cell phones. | 5 | 2 | 10 |
| **Social Media** | Social media can make you a target for threat actors seeking information. Social media patterns of use and location services can be used to infer sensitive information. | 5 | 2 | 10 |
| **Email and telephone** | Email use and phone conversations are vulnerable to disclosure. Do not ‘talk around’ sensitive information. Whenever possible, use secure communication methods. | 4 | 2 | 8 |
|  |  |  |  |  |

The seven risks above are the most dangerous risks we face in our sheltered lab environment. Below is more detail on the top three risks associated with data security, physical security, and passwords.

### Top Risks

#### Data Security

Data security is a top concern for the program because a breach in this area puts the entire program at risk via a loss of contract or a loss of intellectual property. This topic is very broad, but it includes many of the human practices needed to protect both classified and unclassified information in the sheltered lab. There have not been any breaches in this area yet, but there has been a series of events that have highlighted the complacency that has developed in this area.

Training in this area will focus on classification guide usage, the importance of using trusted upload/download procedures, and case studies on how data security efforts have been compromised in other companies and the associated costs. This topic applies to all of our targeted groups, but there needs to be a special emphasis placed on training for I&T since they may not be familiar with proper procedures, and on the algorithms team since they are the most frequent users of the lab.

#### Physical Security

Physical security is an important risk because access control to the lab and computers is a defining requirement of the sheltered analysis environment essential to both the contract and required by regulation. Physical security includes the protection of systems and physical media such as working papers, documents, and CDs. Unprotected physical assets disrupt our ability to protect the information necessary to continue the program comply with federal regulations.

Training for this module includes requirements for opening and closing the lab, authorizing lab access, and physically protecting systems and information. It is especially important to cover the complicated requirements for transporting the lab and using the information systems outside of the sheltered area onsite (such as when a portion of the lab must travel to a government test site). We need to educate users on both Northrop Grumman and government physical security measures. This topic applies to all groups but is especially relevant to the Security Team since they are responsible for the physical security measures of the lab, and the Algorithm Team since they ensure the security of the system when it travels to government test sites.

#### Passwords

Passwords have been a traditional pain point in sheltered lab environments because of the infrequent use by some members (1-2 times a quarter), coupled with the 90-day maximum password age required by DSS. Passwords should not be reused between systems.

Training for this module needs to provide both the requirements for user’s passwords as well as good password management techniques. This module will also include training on how to use our two-factor authentication system and how to reset tokens if needed. This training is necessary for all users, but there is more emphasis on managing 2FA for the Security Team, and more emphasis on best password practices for everyone else.

## 

## Strategies (HOW)

A defense program that cannot protect sensitive information will quickly not be a program at all. All users of the sheltered lab need to understand the criticality of protecting information. Because of company-wide education and training programs, there is some awareness of the importance of information security, but our program needs more specific training to achieve the desired results of mitigating risks mentioned in the previous section. The strategy below outlines how the Security Team will deliver effective training tailored to our user groups. More importantly, our strategy aims to convince users of the importance of security and produce a culture shift rather than merely adding another requirement on their time. The lab security awareness plan is a supplement to the Northrop Grumman security awareness program, so the focus is on areas not covered by the broad company plan. Both the lab and company security plans will work together to achieve the desired goals while reinforcing best practices.

### Overall Engagement Strategy

The overall strategy is to convince users how their daily practices in the lab can have significant security implications. Security is a cornerstone of everything we do as a company and as a program. NGC yearly training establishes a bedrock of security awareness, but our program’s awareness plan will make it applicable to the daily tasks of our lab’s users. We will engage in small groups with lab users to highlight the proper practices, and how following these practices help us to win contracts, maintain an excellent reputation as a program and as a company, and even protects our jobs. Proper security practices exude professionalism while improper practices can cost money, and even cost an employee their job.

### Organizational Culture

The Northrop Grumman Corporation has a unique culture, and our program has its own unique subculture. The best training will use methods that are well received by the target group demographic. Our security awareness program will tailor training both to the general demographic of the program, and the specific sub demographics of the Algorithm Team, Security Team, and I&T Team.

In general, our culture values ingenuity and problem-solving. Many employees within Northrop Grumman have technical degrees and work in an environment surrounded by other people like them. This can create an insular culture where people are not aware of the value of practices that do not align with their specialty. On the other hand, many people in this program have been in the defense contracting industry for over ten years and have a general working knowledge of information security. The security awareness program will seek to bridge this gap by highlighting how applicable information security is to each user group in the lab and empowering users to share experiences and brainstorm solutions to common security challenges. Most NGC employees switch programs every few years; our 30-year-old program is an exception where many members have been here for much longer than average. This has created a subculture of stability within our program that is different from NGC as a whole. Ensuring the program’s stability is an important motivating factor that will make users want to practice good security. The technical background of the members of our program also may incline them more to data-driven presentations rather than roleplaying or storied presentations. All lab members speak American English exclusively for their work at a professional fluency level, so there are no requirements for multilingual training. There are also differences between the user groups in demographics. Some of the differences in training are shown in the table below.

|  |  |  |
| --- | --- | --- |
| **Demographic** | | **Training adjustment** |
| **Algorithm** | Engineers, Masters Degrees, Gen X or Baby Boomer | Printed handouts, classroom presentation with charts, checklists, focus on passwords |
| **Security** | IT & Security, BS, Gen X or Millennial | Print/Email roundtable discussion, logs, collaborative review |
| **I&T** | Millennial or Gen Z | Emailed notes, posters in the lab, video training, focus on |
|  | |  |

### Formal Training Methods

The primary training methods will be a quarterly security lunch-n-learns, fact sheets, handouts, and posters. These materials will be tailored for each of the target user groups depending on their specific risks, demographics, and other needs. The NGC security awareness program already has several videos and interactive yearly and biannual training requirements that cover most of the big topics in security (with associated quizzes), allowing our program’s security awareness program to focus on areas that are unique to our lab environment.

Because of the limited time and resources available for training, we need to communicate key information quickly and consistently. We can make one lunch and learn per quarter mandatory for each of the user groups. With three user groups, this is nine lunch and learns a year - the Deputy Program Manager will fund these lunches and provide an additional incentive to attend security training. The lunch and learns are the best time for a long-form presentation of security practices and trends in the lab. It also is an opportunity for users to ask questions and make suggestions for the program. This is critical to make users feel ownership of the program and a great opportunity for new ideas. For the Algorithm and Security Teams, this lunch will focus on numbers, practices, and checklists. For the I&T team, this will include a short video on applicable security practices and checklists.

Factsheets and handouts will be distributed immediately after lunch and learns to reinforce the training presented and have an accessible copy of any pertinent information. These materials and posters will also be on display in the lab for quick reference. The material for these factsheets will be based on lab SIEM data, DSS audit notes, and observations made by security staff. SANS newsletters, DISA, and NGC infographics will also be used.

### New Hires

New hires are already required to read, sign, and adhere to lab security rules. We will add a personal lab introduction by security personnel to our existing on-boarding process for the lab. This will allow Security Team members to verify that new users understand some of the unique requirements of the lab that may be different from the rest of NGC or even other computer bays within our program. This walkthrough will be added to the existing tracking system for onboarding.

### Branding and Imagery Decisions

Northrop Grumman has strict guidelines for branding, even using company branding for internal training materials. The process to obtain permission to use company branding for our training materials (presentations and handouts) requires a prohibitive amount of paperwork. Our program has its branding that is easier to get permission to use, and it will be used on any internally-developed materials. NGC branding may still be used on any of the security awareness resources that the company makes available for programs to use. These resources are a great no-cost way to get material that may be applicable to training needs.

### Sustainment

For maximum effectiveness, our security awareness program needs to be a consistent fixture in the program. This requires support from users and program managers. We will work on improving and maintaining support from users by soliciting feedback on lunch and learns, and other training materials. It is also important to make sure users feel ownership of the security of the sheltered laboratory. Regular informal interaction with lab users talking about security efforts is key in establishing a sense of mutual ownership; luckily, this is easily achievable due to the small number of people in the lab. Maintaining support from managers will depend on regular communication through the advisory committees. We will be meeting with the advisory committee quarterly and presenting metrics, successes, and challenges. The security awareness program will be sustainable if users feel a sense of ownership, and managers are regularly reminded of its effectiveness.

Meetings with management and the advisory committee will also be a good forum to talk about how training should evolve as the program matures. Feedback from users can be discussed, and training can be modified or improved to meet new needs or preferences. The Deputy Program Manager will present the Program Manager and the government contracting officers with program highlights yearly.

## Metrics

Metrics are essential to measuring the effectiveness of the security awareness program for the sheltered lab. We need to make sure the time, money, and effort being spent is returning a measurable change in user behavior. While many of the culture changes surrounding security practices may be harder to measure, there are still plenty of easy to measure metrics. These metrics can be either compliance or impact related.

Compliance metrics measure if we are doing what we are required to by law, regulation, or program dictate. They do not measure if the training was effective, but it measures if the training happened and who attended. It is important to track these metrics in a verifiable record such as emails, minutes, and sign-in sheets to fulfill audit requirements. Several groups would be potentially interested in these compliance metrics, including NGC ISSM, DoD, DSS, and program leadership.

Impact metrics measure how well our program is changing outcomes. These measure quantitative or qualitative events to determine if training is effective. While these metrics may not be as interesting to auditors, they do tell program leadership that we have reduced the risk of a security incident due to human error. Security incidents do have a measurable impact on the program, and auditors tend to be critical of a program that suffers a security incident. Below is a collection of three different impact metrics that will be tracked by the program.

### Metric 1 - Exposed Devices

Exposed Devices are recorded by security staff or the NGC ISSM when a device is found outside of a locked container or is in the sheltered lab powered on without anyone present. This is also a reportable event if there is any exposed device at the government test site or if there is a mistake in how devices are handled in shipping. These events are logged and reported to the Security Staff; these incidents will be collected monthly by the lab Security Team lead and presented to the advisory committee.

### Metric 2 - Unlogged Information Transfer/Exposure

Transferring information in or out of the sheltered lab requires logging the data in or out, obtaining transfer approval from security staff, and creating appropriately labeled media. It should be easy to trace what was transferred by who, who approved the transfer, and where the media is located. Each week, these three logs are reviewed by security staff to find any inconsistencies. There are also SIEM rules that create alerts on data transfer events (USB, CD, and SSH). Inconsistencies are logged and tracked by the lab Security Team lead.

### Metric 3 - Password Issues

Password reuse, sharing, or compromise are all tracked under the password issues category. These issues cover both memorized passwords and 2FA tokens. All of these issues are tracked by our SIEM and compromise can also be tracked when our users self-report that they have lost their 2FA tokens or forgot their password. These metrics are collected weekly and recorded by the lab security lead. They are also presented quarterly to the advisory committee.

## Appendix A - Learning Objective - Data Security

**Title:** Data Security Learning Objectives

**Target Audience:** Algorithm staff and I&T staff must understand objectives 1-3, security staff must demonstrate objectives 1-5.

**Goal:** Participants will increase the observance of practices that ensure the protection of sensitive lab information. They will learn how to identify relevant classified and sensitive information, and also understand where to look if they have classification questions. Security team members will demonstrate proficiency with processes for moving data in or out of the lab as well as procedures for auditing the lab for information leakage.

**Outcome:** The intended outcome of this learning objective is to lower the risk associated with data security. Data security risks include misclassification, data leakage, data exfiltration and other failures to maintain proper data confidentiality. Data security also includes considerations for maintaining integrity and availability (such as validating that data coming into the lab is clean of malware), but these considerations are secondary to ensuring confidentiality.

**Background:** Data security is the top identified risk for our sheltered lab because compromise of information through loss, theft, or mismanagement can directly lead to a loss of the contract, loss of reputation for NGC, and in cases of neglect - a loss of a job. There have been several instances in the last six months that could have potentially led to a breach of data security. This combination of high probability and impact make mitigating the risk of data security through security awareness training especially important.

**Learning Objective 1 -** Learners will demonstrate how to identify sensitive data.

**Individual metric:** Learners will identify where to find the classification guide for program data and use it to evaluate information classification.

**Organizational metric:** Random sample of generated information for classification correctness.

**Learning Objective 2 -** Learners will demonstrate how to move data into the lab.

**Individual metric:** Learners will summarize the process for moving data out of the sheltered lab, including marking, scanning, and disposing of media.

**Organizational metric:** All three transfer logs agree on who transferred what information into the lab**.**

**Learning Objective 3 -** Learners will show how to prevent information leakage.

**Individual metric:** Learners will Identify common causes of information leakage and list potential mitigations.

**Organizational metric: N/A**

**Learning Objective 4 -** Learners will demonstrate how to move data out of the lab.

**Individual metric:** Learners will demonstrate the entire process for moving data out of the sheltered lab. They will properly check for classification mistakes and forbidden file formats while maintaining an audit log of information moved.

**Organizational metric: See Objective 2**

**Learning Objective 5 -** Learners will demonstrate how to audit the lab for information leaks.

**Individual metric:** Learners will show how to identify signs of unauthorized information leakage on the SIEM dashboard. Learners will access SIEM tools, select proper filters, and identify anomalies that could indicate information leakage.

**Organizational metric:** Trend analysis on weekly SIEM for data movement.