Insider Threat Plan

1.0 PURPOSE

This document applies to Eagle Horizon Group, its wholly-owned subsidiaries, and their members. The Policy directs the creation of an Insider Threat Program and the creation of the Insider Risk Management Group to function as the executive agent of the program. This is a living document and will be updated when changes occur in addressing the never ending threat.

2.0 POLICY STATEMENT

In compliance with National Industrial Security Program Operating Program Manual (NISPOM) Conforming Change 2 and Insider Threat, Eagle Horizon Group, , (EHG), has established an Insider Threat program to deter, detect, and mitigate insider threats and risks to EHG and their clients, information, operations, resources and personnel. The NISPOM outlines: Contractors will establish and maintain an insider threat program that gathers, integrates and reports relevant and available information on potential or actual insider threat in accordance with E.O. 13587. (Obama, Barack. *Executive Order 13587) (NISPOM 1-202)*

The Insider Risk Management Group for EHG will oversee the Insider Threat Program. The Insider Risk Management Group will be led by an appointed Key Management Personnel (KMP) by the Eagle Horizon Group,, Chief Executive Officer. *(NISPOM 1-202a)*

3.0 BACKGROUND

Eagle Horizon Group, (EHG) employees (or Insiders) have authorized access to valuable client, EHG and members' personal information. When insiders choose to exploit this access for personal gain, maliciousness, or retribution for a perceived wrong the inflicted damage can be extensive and costly. Developing a synchronized approach to moderate this vulnerability takes a team effort including support staff, management and vigilant members. (NISPOM Chapter 1-200)

4.0 DEFINITION

An Insider Threat is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system or data and intentionally exceeds or misuses that access in a manner that negatively affects the confidentially, integrity, or availability of the organization's information, operations, resources and systems. For the purpose of this policy, a malicious insider is defined as a current or former employee, contractor, or business partner who meets the following criteria:

- has or had authorized access to an organization's network, system, or data
- has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

Insider threats are influenced by a combination of technical, behavioral, and organizational issues and will be addressed by policies, procedures, and technologies. Accordingly, EHG staff in management, Chief Human Capital Officer, legal counsel, physical security, and information technology (IT) as well as data owners, can

4143 Weeks Drive, Suite B, Vint Hill, VA 20187 www.eagle-horizon.com (540) 326-4542 (540) 326-4546 FAX

all benefit from implementing this policy. Decision makers across the company shall understand the overall scope of the insider threat problem and communicate it to all the organization's employees.

5.0 APPLICATION

All Eagle Horizon Group, employees are responsible for compliance with this policy as well as with all applicable federal, state, and local laws and regulations. The application of this policy must be aligned with the company's Security Plan and Procedures. This policy will become effective as December 1, 2016 and will be made applicable to all employees upon hire.

6.0 RESPONSIBILITIES: (NISPOM Section 1-200)

A. Eagle Horizon Group, CEO

Appointment of Key Management Personnel to oversee the EHG Insider Threat Program. Ensure the appointment of the Insider Threat Program Senior Official is list on the Key Management

B. Threat Program Appointees: (NISPOM 1-202b)

- Insider Threat Program Senior Official (ITPSO)

All appointed members will be required to enroll in the Insider Threat Awareness Course and that of the Counterintelligence Awareness and Security Brief. The Facility Security Officer will monitor to ensure all enrollment into these program and completion certificates are maintained on file and brief the CEO on the status of this required training. The appointees will meet as needed and will conduct an audit as described in Appendix C, at least once a year along with the Defense Security Service Self Inspection. (NISPOM 3-103)

C. Designate an Insider Risk Management Group (IRMG)

Key areas of the groups focus:

- Develops and implements the Insider Threat Plan in compliance with appropriate regulation and/or, guidance.
- Coordinates Insider Threat Plan requirements to include but not limited to collection, reporting, and training.
- Provides oversight and direction to mitigation activities
- Provides resources as required to support the Insider Threat program
- Implement and incorporate the policies and procedures identified in the Insider Threat Plan to protect EHG from insider threats.

Members of the IRMG Group shall focus on areas to ensure implementation of the Insider Threat Program through-out Eagle Horizon. The group shall meet every six (6) months or sooner, if necessary. The group should be comprised of individuals within the corporation holding these key roles below.

- Insider Threat Program Senior Official
- Chief Human Capital Officer
- Chief Information Officer
- Corporate Security Officer
- Facility Security Officer

Chief Human Capital Officer:

- Review insider threat policies and implement across the organization.
- Remind employees of the employee assistance program (EAP) if available.
- Chief Human Capital Officer will be the main point of contact when Human Behavior is involved
- Chief Human Capital Officer will be responsible to properly educate employee that any work produced during employment legally belongs to the organization.
- Chief Human Capital Officer will inform IT, Payroll, and Security when personnel are leaving to ensure proper separation of employees.

Legal:

- Review insider threat policies and discuss any issues that arise and how to avoid them in the future.
- Ensure company is in compliance with all Labor and Employment policies.

Physical Security:

- Review policies and procedures for access to company facilities by employees, contractors, and trusted business partners.
- In addition, review any policies on prohibited devices (USB drives, cameras, etc.).

Data Owners:

Data Owners will be held responsible for the data that is created under their projects and ensure all safeguards are being enforced as prescribed by the governing contract.

• Information Technology:

It is IT's responsibility for protecting data, for knowing where it is and who has access to it.

The IT help desk will remind users of procedures for recognizing viruses and other malicious code. IT will instruct all users which devices are prohibited or permitted for authorized use on the various information systems within the organization.

D. Employee Reporting Requirements (NISPOM 1-304)

Eagle Horizon employees, regardless of clearance status, are required to report certain events that; 1) have an impact on the status of the company's Facility Clearance (FCL); 2) impact the status of an employee's personnel security clearance (PCL); 3) affect proper safeguarding of classified information; or 4) indicate classified information has been lost or compromised. 5.) Insider Threat Behaviors as indicated in Appendix A. All cleared employees who have been granted a government security clearance must be aware of their responsibilities for reporting pertinent information to the Facility Security Officer (FSO) as required by the terms of National Security

Program Operating Manual (NISPOM) and the contract requirements for which they are cleared. Eagle Horizon is obligated and responsible for providing complete information and shall submit reports to the U. S. Government as specified in this policy.

Employees need to understand that the organization uses established policies and procedures, applied non-arbitrarily and without personal judgment, and that managers will respond to security issues fairly and promptly and without discrimination.

Confidential reporting will be enforced that allows employees to report suspicious events without fear of retaliation or repercussion, circumventing the cultural barrier against whistle blowing.

Employees can make their report to the Facility Security Officer, or to the Chief Human Capital Officer via electronic mail, facsimile, telephone, or in person. Telephonic or in-person reporting must be followed by a written report. All information about the incident(s) or event(s) should be reported as soon as possible.

If employees are in doubt as to whether a behavior, incident, or event should be called to the attention of the FSO, they need to REPORT IT! The FSO is in the best position to make a determination of the risks and to help mitigate or resolve them. Employees are reminded they can make a report to the Defense Security Service Hotline at 1-800-424-9098 as well.

7.0 SAFEGUARDS

7.1 In General. Eagle Horizon will maintain appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and accessibility of all company records consistent with the requirements of these NISPOM and National Security Directives and Policies and to safeguard Controlled Unclassified Information and that of any classified information from intentional and unintentional non-permissible uses and disclosures. These safeguards will supplement and be consistent with security measures taken by Eagle Horizon.

7.2 General Safeguards.

Eagle Horizon will employ safeguards that include the following:

a. Eagle Horizon will restrict access to all client files pertaining to only the workforce members of Eagle Horizon, the client and authorized Subcontractors of Eagle Horizon.
b. Eagle Horizon will store files contained in a covered location (i.e., such as a file folder).
c. Eagle Horizon will store files in a secured location when not in use (i.e., locked room or file cabinet).
d. Eagle Horizon will use reasonable safeguards so that computer screens will not be visible to unauthorized persons, including locking down computer workstations when not in use or when leaving the workstation by activating a password protected screen saver and clearing personal information and sensitive documents from the computer screen when not actually being used.
e. Eagle Horizon will keep firewalls in place.
f. Eagle Horizon will keep a Virtual Private Network (VPN) in place.
g. Prior to discarding unclassified or sensitive information Eagle Horizon will securely destroy by, shredding documents or destroying hardware that contain sensitive information so that they cannot be read or reconstructed. Sensitive Information stored on digital copiers or other devices must be removed or destroyed before the device is resold, returned at the end of the lease or otherwise no longer under the control of Eagle Horizon. Shred bins are available throughout Eagle Horizon offices.
h. Eagle Horizon will not hold phone conversations or other discussions involving sensitive or controlled unclassified information in areas where unauthorized persons may overhear. Phone conversations should not be held on speakerphone, unless everyone within listening distance is an authorized recipient.

3. Facsimile Safeguards. Eagle Horizon will take reasonable steps to send and receive facsimile transmissions securely, including the following safeguards:

a. Only sending by fax when mail, encrypted e-mail or hand delivery are not feasible.

b. Notifying the recipient and double checking fax numbers before dialing.

c. Using the Eagle Horizon standardized fax cover sheet that includes a confidentiality statement and a request that any erroneous recipient destroy or return the fax.

d. Picking up incoming faxes from the fax machine in a timely manner.

e. When sending a fax, remaining at the fax machine until the fax has been scanned completely and not using a fax machine that is accessible to the public.

f. Not leaving faxes to be sent or that have been sent at the fax machine unattended.

g. If aware of a misdirected fax, contacting the recipient and asking them to discard the misdirected fax (and reporting the incident immediately to the FSO).

h. Locating fax machines in secure areas not accessible to the general public or unauthorized staff.

4. E-mail Safeguards. The minimum necessary PII will be sent via e-mail. Any PII transmitted by email will be protected by encryption (secure email) to prevent inadvertent disclosure. An e-mail signature block will be appended to all external recipients stating the confidentiality of the information and what to do if it is received inadvertently. Any Eagle Horizon workforce member who becomes aware of a misdirected e-mail that contains PII must notify the FSO immediately.

The e-mail system and all messages generated or handled by e-mail, including backup copies, are property of Eagle Horizon. E-mail users have no right to privacy in their use of the computer system, including e-mail. Eagle Horizon may monitor the content and usage of the computer system, including e-mail, at any time and for any reason.

7.3 Authorizing Access.

Before granting access to Eagle Horizon systems containing sensitive information or controlled unclassified information to a workforce member, Eagle Horizon will perform a criminal background check of any non-cleared workforce member and evaluate the results to ensure that the workforce member would not pose a risk to the privacy and security of any proprietary and sensitive information. Such background checks should be performed (a) upon initial hire and (b) thereafter, on an annual basis. For new workforce members, the FSO or the applicable supervisor will determine the appropriate level of access in compliance with the NISPOM and Government Contracts. For new Subcontractors, the FSO and CIO must be notified of any Subcontractor requiring access to Eagle Horizon's facilities or information systems to ensure that only appropriate access is permitted consistent with Policy.

8.0 Eagle Horizon Approach to Reducing the Insider Threat

8.1 Before Employment - Hiring Process

Eagle Horizon Group uses XCELHR to conduct all background checks as necessary. Eagle Horizon will take into consideration legal requirements (e.g., notification to and consent from the candidate) when creating a background-check. Eagle Horizon will implement and ensure all employees, contractors, and trusted business partners sign nondisclosure agreements (NDAs) upon hiring and termination of employment on contracts.

Prior to making any employment decisions based on background information, Eagle Horizon shall consider legal guidance, including the Equal Employment Opportunity Commission's (EEOC's) best practices and state and local regulations limiting the use of criminal or credit checks. Eagle Horizon will use background information lawfully, with due consideration to the nature and duration of any offense, as part of a Risk-based

decision process to determine the employee's access to critical, confidential, or proprietary information or systems. Eagle Horizon will take into consideration of assigning risk levels to all positions and more thoroughly investigate individuals applying for positions of higher risk or that require a great deal of trust [NIST 2009].

8.2 During Employment

Periodic reinvestigations may be warranted as individuals move to higher risk roles within the organization, again complying with all legal requirements.

.

Eagle Horizon understands that malicious insiders have used IT to modify, add, or delete organizational data, without authorization and for personal gain. IT is also used to steal information that leads to fraud (e.g., identity theft, credit card fraud). Sudden changes in an employee's financial situation, including increased debt or expensive purchases, may be signs of potential insider threat. Eagle Horizon will consult with legal to ensure we are in compliance with employment laws, such as employee notifications, prior to taking any adverse action against the employee.

If an employee exhibits concerning behavior, Eagle Horizon will respond with due care. Disruptive employees should not be allowed to migrate from one position to another within the enterprise and evade documentation of disruptive or concerning activity. Eagle Horizon will also treat threats, boasts about malicious acts or capabilities. In general, Eagle Horizon will reach out to help any employee resolve workplace difficulties. Once Eagle Horizon identifies an employee's concerning behavior, it may take several steps to manage the risks of malicious activity. First, Eagle Horizon will evaluate the employee's access to critical information assets and level of network access. The company will carefully review logs of event activity by the employee. Meanwhile, the employees will be given the option to enroll into the EAP with options for coping with issues causing the behavior, which will be held in confidence.

Eagle Horizon will consult with Legal Counsel to ensure all monitoring activities are within the bounds of law. For instance, private communications between employees and their doctors and lawyers should not be monitored. Additionally, federal law protects the ability of federal employees to disclose waste, fraud, abuse, and corruption to appropriate authorities. For the same reason, Eagle Horizon will not deliberately target an employee's emails or computer files for monitoring simply because the employee made a protected disclosure. [NIST 2012].

8.3 Reports to be Submitted by EHG to the U.S. Government (NISPOM 1-300).

8.3.1 Adverse Information. EHG shall report adverse information regarding it's' employees who are cleared for a government security clearance. Reports will not be based on rumor or innuendo. The subsequent termination of an employee does not obviate the requirement to submit this report. This report shall be submitted to the respective government agency or department which the employee's security clearance is granted.

8.3.2 Suspicious Contacts. EHG shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported to the U.S. Government.

8.3.3 Change in Cleared Employees Status. EHG shall report the following information regarding employees who possess a security clearance:

1. Their death
2. Change in name
3. Termination of employment
4. Change in citizenship
5. The possibility that their access to classified information has been reasonably foreclosed

8.3.4 Citizenship by Naturalization. EHG shall report if a non-U.S. citizen employee granted a Limited Access Authorization (LAA) becomes a citizen through naturalization.

8*.3.5 Employees Desiring Not to Perform on Classified Work*. EHG shall report that an employee no longer wishes to be processed for a clearance or to continue an existing clearance.

8.3.6 Standard Form (SF) 312. EHG shall report to the U.S. Government any refusal by an employee to execute the "Classified Information Nondisclosure Agreement" (SF 312).

8.3.7 Change in Cleared Employees Status. EHG shall report the following information regarding employees who possess a security clearance:

1. Any change of ownership, including stock transfers that affect control of the company.
2. Any change of operating name or address of the company or any of its cleared locations.
3. Any change to the information previously submitted for key management personnel including, as appropriate, the names of the individuals they are replacing. In addition, a statement shall be made indicating (a) whether the new key management personnel are cleared, and if so, to what level and when, their dates and places of birth, social security number, and their citizenship; (b) whether they have been excluded from access; or (c) whether they have been temporarily excluded from access pending the granting of their clearance. A new complete listing of key management personnel need be submitted only at the discretion of EHG and/or when requested by the U.S. Government.
4. Action to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the FCL.
5. Any material change concerning the information previously reported by the contractor concerning foreign ownership, control or influence (FOCI). This report shall be made by the submission of a Certificate Pertaining to Foreign Interests. When submitting this information, it is not necessary to repeat answers that have not changed. When entering into discussions, consultations or agreements that may reasonably lead to effective ownership or control by a foreign interest, EHG shall report the details by letter. If EHG has received a Schedule 13D from the investor, a copy shall be forwarded with the report.

8.3.8 Change in Cleared Employees Status. Any change in the storage capability that would raise or lower the level of classified information the facility is approved to safeguard. Any emergency situation that renders the facility incapable of safeguarding classified material

8.3.9. Security Equipment Vulnerabilities. Significant vulnerabilities identified in security equipment, intrusion detection systems (IDS), access control systems, communications security (COMSEC) equipment or systems, and information systems (IS) security hardware and software used to protect classified material.

8.3.10. Unauthorized Receipt of Classified Material. Unauthorized material will be promptly reported The report should identify the source of the material, originator, quantity, subject or title, date, and classification level.

8.3.11. Employee Information in Compromise Cases. When requested by the U.S. Government, information concerning an employee when the information is needed in connection with the loss, compromise, or suspected compromise of classified information.

8.3.12. Disposition of Classified Material Terminated from Accountability. When the whereabouts or disposition of classified material previously terminated from accountability is subsequently determined

8.3.13. Foreign Classified Contracts. Any pre-contract negotiation or award not placed through a government contracting agency that involves, or may involve: (1) the release or disclosure of U.S. classified information to a foreign interest or (2) access to classified information furnished by a foreign interest.

8.3.14. Reports of Loss, Compromise, or Suspected Compromise**.** Any loss, compromise or suspected compromise of classified information, foreign or domestic, shall be reported to the U.S. Government. Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise. If the facility is located on a Government facility, the report shall be furnished to the U.S. Government through the Commander or Head of the host installation.

8.3.15.

1. ***Preliminary Inquiry***. Immediately on receipt of a report of loss, compromise, or suspected compromise of classified information, the EHG shall initiate a preliminary inquiry to ascertain all of the circumstances surrounding the reported loss, compromise or suspected compromise.

2. ***Initial Report.*** If EHG's preliminary inquiry confirms that a loss, compromise or suspected compromise of any classified information occurred, EHG shall promptly submit an initial report of the incident unless otherwise notified by the U.S. Government. Submission of the initial report shall not be deferred.

3. ***Final Report.*** When the investigation has been completed, a final report shall be submitted to the U.S. Government. The report shall include:

a. Material and relevant information that was not included in the initial report;

b. The name and social security number of the individual(s) who was primarily responsible for the incident, including a record of prior loss, compromise, or suspected compromise for which the individual had been determined responsible;

c. A statement of the corrective action taken to preclude a recurrence and the disciplinary action taken against the responsible individual(s), if any; and

d. Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise occurred or did not occur.

e. EHG has no safeguarding at this time. Policy will be updated upon being granted safeguarding requirements to ensure handling, storage, processing and destruction of classified information is included in this policy as well addressed in the company Standard Practice and Procedures.

8.3.16 Individual Culpability Reports. (NISPOM 1.304) EHG has established policies and enforces those policies that provide for appropriate administrative actions to be taken against employees who violate requirements set forth in this policy. EHG has established a graduated scale of disciplinary actions in the event of employee violations or negligence. A statement of the administrative actions taken against an employee shall be included in a report to the U.S. Government when individual responsibility for a security violation can be determined and one or more of the following factors are evident:

1. The violation involved a deliberate disregard of security requirements.

2. The violation involved gross negligence in the handling of classified material.

3. The violation involved was not deliberate in nature but involves a pattern of negligence or carelessness.

The gradual scale of discipline is included in the HR Handbook and that of the Security SPP.

8.4 Termination Process.

Eagle Horizon termination procedure will be implemented to reduce the risk of damage from former employees. Termination procedures should ensure that the former employee's accounts are closed, his or her equipment is collected, and the remaining personnel are notified. Proper account and inventory management processes will be created to reduce the insider threat risk when an employee separates from the company.

In preparation of an employee's departure, Eagle Horizon will take action to address a number of areas before the employee's last day. At a minimum, a termination checklist will be developed to include the task, who should complete the task, who should verify task completion, when the task needs to be completed by, and a signature line for the initials of the person completing the task. The completed checklist should be returned to Chief Human Capital Officer before the employee leaves the organization.

Below is a list of areas that Eagle Horizon will address during a termination and include on a termination checklist:

• Manager:
− Ensure an exit interview is scheduled and completed by the next higher level of Management or Chief Human Capital Officer
− Provide final performance appraisal feedback.
− Collect final timesheets.
− Determine where final paycheck is to be mailed.

• Finance department:
− Ensure employee returns company credit cards, calling cards, purchasing cards, and so on.− Close the accounts.

• CIO:

− Notify systems administrators of account suspension and archiving. The system or network administrator should do the following:

 Terminate all accounts (VPN, email, network logins, cloud services, specialized applications, company-owned social media site accounts, backup accounts).

 For departing privileged users, change all shared account passwords, service accounts, network devices (routers, switches, etc.), and so on.− Collect remote access tokens (two-factor authentication devices).
− Update access lists to sensitive areas (server rooms, data centers, backup media access, etc.).
− Remove employee from all distribution lists and automated alerts.

− Ensure employee returns all equipment, such as software, laptop, tablet, netbook, and smartphone. − Verify returned equipment against inventory.

• Facility Security Office:
  − Ensure employee returns any company-owned or controlled documents.
  − Collect identification badge, keys, access cards, parking pass, and so on. − Provide security debriefing.

• Chief Human Capital Officer
  − Obtain forwarding mailing address.
  − Complete separation paperwork.
  − Notify organization of separation.
  − Reaffirm any IP and nondisclosure agreements.
• Facilities:
  − Collect desk phone.
  − Clear work area.

As part of the separation process, Eagle Horizon must collect its physical property, including badges, access cards, keys, two-factor authentication tokens, mobile devices, and laptops. Any of these items, if not returned, may enable the former employee to attack the company. Collecting these items cannot completely prevent such attacks, but it will aide against any attacks.

Eagle Horizon next step in the separation process is to reaffirm with the departing employee any agreements about IP and nondisclosures. This is an opportunity to remind the employee about his or her obligations to the company even after separation.

9.0 **Insider Threat Training** (NISPOM 3-103)

EHG Threat Program Appointees Training Program will include:

A. Counterintelligence and security fundamentals including applicable legal issues
B. Procedures for conducting insider threat response actions
C. Laws and regulations on gathering, integration, retention, safeguarding and use of records and data and the consequences of misuse of such information
D. Legal, civil liberties and privacy policies

Specific insider threat employee related training will include:

A. The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee
B. Methodologies that adversaries use to recruit trusted insiders
C. Indicators of insider threat behavior and how to report such behavior
D. Counterintelligence and security reporting requirements

Training must be satisfactorily completed within 30 days of initial employment or prior to being granted access to classified information, and annually thereafter. EHG's Facility Security Officer is responsible for establishing a system to validate and maintain records of all cleared employees who have completed the training.

10. **Contact Information**

If you have any questions about this policy, please contact:

Eagle Horizon Facility Security Office at (540) 326-4542

ADMINISTRATION

Effective Date: December 1, 2016

Approving Authority:

Rae Ohlert
Chief Executive Officer
4143 Weeks Drive, Suite B
Vint Hill, VA 20187

References:

[DHS 2011]
Department of Homeland Security. *National Cyber Security Awareness Month.* http://www.dhs.gov/files/programs/gc_1158611596104.shtm (2011).

[GAO 2010]
U.S. Government Accountability Office. *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing* (GAO-10-513). U.S. Government Accountability Office, 2010. http://www.gao.gov/new.items/d10513.pdf

[Infosecurity 2010]
Infosecurity. "Air Force's Banning of Thumb Drives Temporary Solution to WikiLeaks," *Infosecurity* (online, December 17, 2010). http://www.infosecurity-magazine.com/ view/14762/air-forces-banning-of-thumb-drives-temporary-solution-to-wikileaks/

[NISPOM]
National Industrial Security Program Operating Manual

[NIST 2009]
National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems and Organizations* (NIST SP 800-53, Rev. 3). National Institute of Standards and Technology, 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/ sp800-53-rev3-final.pdf

[NIST 2010a]
National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems* (NIST SP 800-37, Rev. 1). National Institute of Standards and Technology, 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/

[NIST 2010b]
National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems and Organizations* (NIST SP 800-53A, Rev. 1). National Institute of

Standards and Technology, 2010. http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/

[NIST 2012]
National Institute of Standards and Technology. *Risk Management Framework (RMF) Overview.* National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Center, 2012. http://csrc.nist.gov/groups/SMA/fisma/framework.html

[Obama 2011]
Obama, Barack. *Executive Order 13587 -- Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*.
The White House, Office of the Press Secretary. http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

APPENDIX A.

INSIDER THREAT REPORTABLE BEHAVIORS

As mandated by the new National Industrial Security Program Operating Manual (NISPOM) change 2, all individuals employed by or with Eagle Horizon must immediately report any of the following activities, indicators, or behaviors to your Manager, the Facility Security Officer, the Insider Threat Program Senior Official (ITPSO) or the Chief Human Capital Officer.

Table 1. Reportable Contacts, Activities, Indicators, and Behaviors

1.	When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against facilities, organizations, personnel, or information systems. This includes contact through social networking sites that are not related to official duties.
2.	Attempts by anyone, regardless of nationality, to obtain or acquire unauthorized access to classified or sensitive information in the form of facilities, activities, personnel, technology or material through any of the following methods: questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (including electronic correspondence) or automated systems intrusions.
3.	Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
4.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
5.	Acquiring, or permitting others to acquire, unauthorized access to classified information systems.
6.	Attempts to obtain classified information by an individual not authorized to receive such information.
7.	Persons attempting to obtain access to information inconsistent with their duty requirements.
8.	Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
9.	Discovery of suspected listening or surveillance devices in classified or secure areas.
10.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
11.	Discussions of classified information over a non-secure communication device.
12.	Reading or discussing classified information in a location where such activity is not permitted.
13.	Transmitting or transporting classified information by unsecured or unauthorized means.
14.	Removing or sending classified material out of secured areas without proper authorization.
15.	Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.

16.	Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
17.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
18.	Unwarranted work outside of normal duty hours.
19.	Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
20.	Attempts to entice personnel or contractors into situations that could place them in a compromising position.
21.	Attempts to place personnel or contractors under obligation through special treatment, favors, gifts, or money.
22.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
23.	Requests for information that make an individual suspicious, to include suspicious or questionable requests over the internet or social networking sites.
24.	Trips to foreign countries that are: a. Short trips inconsistent with logical vacation travel or not part of official duties. b. Trips inconsistent with an individual's financial ability and official duties.
25.	Personnel who are in contact with any official or citizen of a foreign country when the foreign official or citizen: a. Exhibits excessive knowledge of or undue interest in personnel or their duties beyond the normal scope of friendly conversation. b. Attempts to obtain classified or unclassified information. c. Attempts to place personnel under obligation through special treatment, favors, gifts, money or other means. d. Attempts to establish business relationships that are outside the scope of normal official duties.
26.	Incidents in which personnel or their family members traveling to or through foreign countries are contacted by persons who represent a foreign law enforcement, security or intelligence organization and a. Are questioned about their duties. b. Are requested to provide classified or unclassified information. c. Are threatened, coerced or pressured in any way to cooperate with the foreign official. d. Are offered assistance in gaining access to people or locations not routinely afforded Americans.
27.	Unexplained or undue affluence. a. Expensive purchases an individual's income does not logically support. b. Attempts to explain wealth by reference to inheritance luck in gambling, or a successful business venture. c. Sudden reversal of a bad financial situation or repayment of large debts.
28.	Contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which: a. Illegal or unauthorized access is sought to classified or otherwise sensitive information. b. The employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.
29.	Any contact with the media where the media seeks access to or results in the unauthorized disclosure of classified information, unclassified, or other information not approved for public release.

30.	Arrests, charges, convictions, and criminal court appearance (with the exceptions of a summons for jury duty or to appear as a witness or provide other testimony when the individual is not being charged or otherwise being prosecuted). Traffic infractions where the fine was less than $300 and did not involve alcohol or drugs are not reportable. All reports should include dates, jurisdiction, name of the court, nature of the issue, and disposition, if available. Changes in the status of any previously reported court involvement shall also be promptly reported.
31.	Adverse changes to financial status to include, but not limited to, garnishments, foreclosures, liens, judgments, delinquent taxes, and/or bankruptcy filings.
32.	Any hospitalization for a mental health condition.
33.	Use of or involvement with illegal drugs or controlled substances, and/or the misuse of prescription/legal drugs or dangerous inhalants.
34.	Voluntary or involuntary treatment for abuse of alcohol or illegal use of controlled substances.
35.	Close and continuing association with foreign nationals.
36.	Unwillingness to comply with rules and regulations, or to cooperate with security requirements.
37.	Alcohol abuse.
38.	Apparent or suspected mental or emotional condition where there is reason to believe the condition may affect the individual's judgment, reliability, or ability to protect classified information.
39.	Criminal conduct.
40.	Any activity that could constitute a conflict of interest with U.S. Government employment.
41.	Misuse or abuse of U.S. Government property or information systems.

Table 2. Reportable Suspected Terrorism or Work Place Violence Contacts, Activities, Indicators, and Behaviors

1.	Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2.	Advocating support for a known or suspected international terrorist organizations or objectives.
3.	Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4.	Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5.	Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
6.	Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7.	Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
8.	Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9.	Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.

10.	Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.
11.	Possessing weapons in the work place.
12.	Threatening to kill or harm supervisors, co-workers or anyone else within or outside of the work place.
13.	Sending emails or posting on social media sites threatening communications against supervisors, co-workers or anyone else within or outside of the work place.

Table 3. Reportable Behaviors Associated With Cyberspace Contacts, Activities, Indicators

1.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of U.S. Government information.
2.	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3.	Network spillage incidents or information compromise.
4.	Use of account credentials by unauthorized parties.
5.	Tampering with or introducing unauthorized elements into information systems.
6.	Unauthorized downloads or uploads of sensitive data.
7.	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	Unauthorized e-mail traffic to foreign destinations.
11.	Denial of service attacks or suspicious network communications failures.
12.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13.	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14.	Data ex-filtrated to unauthorized domains.
15.	Unexplained storage of encrypted data.
16.	Unexplained user accounts.
17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19.	Malicious codes or blended threats such as viruses, worms, Trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

APPENDIX B.

INSIDER RISK EVALUATION AND AUDIT TOOL

Eagle Horizon Risk Evaluation and Audit Tool will be submitted under separate cover due to volume and size of document. This plan will be made available on line.