**Assessment of Transport Security Controls**

**The following table is a tool for the TSUSG Priority 6 group to assess the effectiveness or absence of transport security controls intended to mitigate insider threat risks and to identify improvement options.**

The table will be broken down by type of measure and the objective of the measure.

The term **‘preventive measures’** is used to describe measures to prevent or remove possible insider threats, to minimize threat opportunities, or to prevent a malicious act from being carried out.

The term **‘protective measures’** is used to describe measures to detect, delay and respond to malicious acts that are carried out and to mitigate or minimize their consequences.

| **Control Objective** | **Measure** | **Effectiveness of Measure / Issues** | **Improvement Options** |
| --- | --- | --- | --- |
|  | | | |
|  | **1.0 - Preventative Measures** | |  |
| 1.1 Trustworthiness and Reliability of employees, students, and contractors | Persons are required to obtain a security clearance (initial onboarding) | Persons required to obtain a government security clearance which will include completion of thorough background checks that provide the organization with a sense of trustworthiness and reliability for employees. Background checks, including financial standing, prior criminal associations, substance abuse, and extremist ideology, are examples of measures which provide a full picture of a person’s integrity.  An issue is that DOT/FMCSA does not require a high level of rigor about background checks due to co-regulation of NRC requirements.  Background checks vary across commercial and government organizations, thus potentially missing key indicators for new employees.  Only a measure of recorded criminal activity and financial record is typically considered without a more thorough background check. | Requiring subcontractors to adopt more stringent background investigations on employees can be challenging, time-consuming, and financially burdensome for organizations that do not have needed resources in place. We have to be careful about adding new requirements on subcontractors for fear of losing them. Very few qualified vendors can prepare devices for shipment. In some instances, vendors are uniquely qualified to work on specific devices.  Agencies completing background checks, i.e., municipal, state, and federal, should integrate to cross-reference civil violations with other adjudicative criteria.  Consider upgrading to new technologies, such as collecting electronic fingerprints. |
| Routine Reinvestigations-every 5 years, current employees, students, and contractors are reviewed for changes to their records, such as criminal or financial. This does not include an investigation-for-cause. | 5-year updates for employees with security clearances, unless a more rigid program is in place to reduce the frequency of checks from 5-years to 2-years, for example. This can be costly for organizations that do not have the personnel security infrastructure in place.  5 Years is a long period of time between initial and recheck. | Emphasize peer-and self-reporting requirements. However, recognize that peer reporting can be abused or avoided due to work-place dynamics.  Midpoint checks every two years or more frequently at the employer’s discretion.  Employers should establish a self-reporting policy. Employee must self-report any civil or criminal status. |
|  | | | |
| 1.2 Information Protection | Practice “need to know” and limit distribution of information. Only provide what is needed for that person to perform their task, when possible. | Extremely important action but can sometimes be difficult to control. This is where a good trustworthiness program is important, but still, vulnerabilities must be evaluated. There may be instances where we are asked to provide more information to regulatory and site personnel to ensure transparency of the operations. This seems like it could conflict with good security practices, but it is about making sure only people with a need to know are involved and are aware of the sensitive nature of the information. A national laboratory has a roles and responsibilities document that the site and the subcontractor sign and it has a section on this topic.  Everyone thinks they “need to know” outside of organization - no way to control | Ensure good operations security (OPSEC) awareness  Personnel having access to sensitive information are trained and aware of the requirements. Give examples of good OPSEC and bad OPSEC.  For single contractual transport activities, signed non-disclosure agreement (NDA) should be implemented. |
| Document Transmission / communication protocols, including encryption, password protection, etc. | Encryption, secure fax, and password protection are great controls / Must ensure equipment is compatible across the board.  Not all organizations have compatible encryption | Test transmission systems between pertinent organizations periodically and/or send “test” messages first, get confirmation, prior to sending the “real” information. Only provide information that is necessary for the task.  Use coded message systems, (playbook) |
| Voice communications protocols – use of radios with drivers and escorts. Use of radios with encrypted comms, etc. | Using robust and secure communications is an important element for security and can be directly related to the ability of responders to respond effectively. | Train personnel to communicate minimal information during transit. If available and cost effective, incorporate robust equipment, such as frequency hopping, connectivity to trunk lines or use of repeaters. Of course, back-up communications equipment is important.  Keep comms short, use multiple comms, use point to point radio systems with short range |
| 1.3 Security Awareness | Training on policy and procedures and threats (w/ reoccurring training cycles) | Very important and effective as long as management and employees understand the implications and take elements of good security practices seriously. | Encourage security awareness training. Incorporate case studies and mock exercises that are best for driving home some of these points. Recurring read-only training will not likely be effective. |
|  | | | |
| 1.4 Physical Access Controls | Limit physical access to information/shipments/storage of cargo only to those with an operational requirement | So important but needs to be managed and updated as needed by trusted individuals to ensure physical access is strictly controlled. | Minimize personnel having access to information. Employ two-person control for those requiring access to sensitive materials and storage areas. |
|  | | | |
| 1.5 Situational Awareness  *(note: not really sure about this one. It is about reducing opportunity for an insider to take advantage of external events…)* | Sharing relevant threat and incident information between stakeholder groups | Always good to share lessons learned but minimize distribution to personnel with need to know. | Limited distribution |
| Route and schedule planning in consideration of events or anticipated events | Route planning is the carrier’s responsibility, so hopefully these issues are considered. / For overweight permitted shipments, there are sometimes few options. | Have secondary routes preplanned if needed. Sometimes things are unavoidable like road construction, accidents, etc., but the idea is always to keep the shipment moving if possible and try best to avoid situations that could put the shipment at risk.  Only share with drivers, control centers and required state/federal/local authorities. |
|  | | | |
| 1.6 Business Partnerships | Audit supply chain partners to ensure a minimum-security requirement is being met | NRC/Agreement States perform assessments on subcontractors that prepare devices for shipment. One national laboratory reviews these thoroughly before considering using vendors for the work. For carriers, the referenced laboratory, institutionally, relies on evaluations performed by the DOE’s Motor Carrier Evaluation Program, or MCEP.  Security awareness training may not meet current federal programs  Be aware of weaknesses of supply chain partners in auditing measures | Work with supply chain partners by implementing security awareness training  Members should be part of the Canadian Customs-Trade Partnership Against Terrorism Program, or CTPAT.  Integrate training and awareness programs across all functional groups where possible. |
|  | **2.0 - Protective Measures** | |  |
| 2.1 Trustworthiness and Reliability of employees, student and contractors  (Detection and Response) | Behavioral Observation Programs | Extremely important, but sometimes can be difficult to implement. Peer reporting can be difficult because of employee fear of retribution. Employees who have a concern about someone may take some time to report because they tend to think about their consequences, thus timeliness could be directly related to increased risk.  Hard to do for remote workers  For some personnel, this is managed through our clearance/clearance re-investigation and insider threat mitigation programs; however, we must be careful implementing specific new requirements for subcontractors and carriers, as this could be challenging. Must recognize that peer reporting can be abused or avoided due to work-place dynamics. | Review if behavioral observation policies are in place for subcontractors and carriers.  Awareness training to identify key indicators. Stress importance of consequences if reporting is not timely.  Review behavioral observation programs to train peers and managers to identify red flags when there is no face to face. |
| Reinvestigation due to red-flag behaviors, etc. | Must be timely. Requires management buy-in and a methodical/sensitive approach.  Requires right people to report red flags in time sensitive manner |  |
| Procedures for review of red-flag behaviors, including review and assessment by trained, multi-function team | Procedures and checklists are important for documentation of a program and to ensure that assessments are done properly and methodically. Some organizations may not have procedures in place. |  |
|  | | | |
| 2.2 Protection of Information (Detection and Response) | Cyber security program, implementing industry best practices & framework across company (i.e. SANS/NIST) |  |  |
| Cyber security measure to detect unauthorized access |  |  |
| Cyber security measures to detect data exfiltration |  |  |
| Response to evidence of information security breach | Needs multidisciplinary team to determine severity of information breech |  |
|  | | | |
| 2.3 Security Awareness  (Detection and Response) | State and local law enforcement agency awareness training on radiological threats, radiation safety, etc. | Contract drivers may not be knowledgeable on radiological threats or radiation safety issues regarding detection and response. |  |
|  | | | |
| 2.4 Communications  (Response) | Pre-established communications protocols within and between response groups | May temporarily lose communications because of poor reception in different areas while traveling | Always have back-up communications for redundancy. Identify dead spot areas prior to commencing shipment and plan for possible loss of comms. |
| Availability and sharing of relevant shipment information for the response | More information sharing would likely be required during a response. The responsible organization for a shipment may have specific requirements for managing message distribution in the event of an emergency. | Must be willing to accept that response personnel need information relevant to the type of response. Designate a point of contact who has authority to share information to response personnel as needed. Recommend table-top exercises as part of a liaison program with first responders. |
|  | | | |
| 2.5 Physical Access Controls  (Detection and Response) | Monitoring of trucks and/or transport packages (GPS/Geofencing) | Good for tracking but GPS signals could be jammed or disabled. Poor quality GPS signals can also be a cause for weak reception if not calibrated properly | Use back-up or independent system, such as RFID tags on packages. Any tracking system must be tested and proven reliable. |
|  | | | |
| 2.5 Physical Access Controls | Manage, monitor, & audit access privileges to sensitive areas where information and/or product is stored | At most DOE high hazard, high consequence facilities, proper access controls are managed and routinely updated by facility managers. Privately run facilities (hospitals, etc.) manage their access control based on NRC/Agreement State requirements. ORS/NA-20 likely cannot control how access control is managed at private facilities. | Security awareness training for facility managers to ensure access if routinely evaluated. |