TRANSPORT SECURITY DISCUSSION POINTS

Thoughts on Best Practices for Governor's Designees

Regulators (Governor's designees) are automatically given access to sensitive information because of their position (primary distribution). This information includes routing, scheduling, isotopes, and quantity of radioactive material in the shipment. This information may be distributed (secondary distribution) to fusion centers, state police, response agencies, and others. Additional distribution (tertiary) may also occur if the secondary recipients further distribute the information.

Does your State have a dedicated process for secondary distribution? If yes, please consider providing responses to the following or a generalized procedure for the process:

Is all the original information provided to the Governor's designee forwarded to all recipients in the secondary distribution? If not, what are the factors that influence the distribution?

Is there a vetting process to ensure the recipients of the information are trustworthy and reliable?

Once the material is transmitted, is there a sufficient security culture or practices to maintain the confidentiality of the information for the short time that the knowledge is relevant?

Do you know if the information is distributed further (tertiary distribution)?

For a tertiary distribution, is all the original information provided? If not, do you know the factors that influence the distribution?

Is there a periodic review of those receiving the information (secondary and tertiary) to ensure they still have a need to know?

What is the method for distribution of the information? Are there security standards used for the distribution (i.e., Federal Information Processing Standard)?

How should relationships be established and/or maintained by the Governor's Designee and those recipients that receive sensitive information?

Would memorandums of understanding (MOU) address employee turnover and be beneficial to maintain continuity of processes and enhanced security requirements during transport of Cat. 1 sources?

If an MOU or similar protocol is implemented:

Should there be a notification process if sensitive information is compromised or an insider threat has been identified? How will corrective measures be implemented and verified?

How should an organization that handles sensitive information provide appropriate initial and refresher training to its workforce?