UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

JUL 3 1 2018

MEMORANDUM

SUBJECT: Final Response to the OIG's Management Alert: To Minimize Risk of
Environmental Harm, the Security Categorization of Electronic Manifest System
Data Needs to Be Re-Evaluated, Report No. 18-P-0217, June 21, 2018

FROM: Barry N. Breen
Acting Assistant Administrator

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations in the subject
Management Alert. The following is our further response to the Management Alert, which
follows our interim response sent to you on June 29, 2018 and the exit conference held on July 9,
2018. The Office of Land and Emergency Management (OLEM) agrees with the three
recommendations in the Management Alert. For those recommendations, we have provided
intended corrective actions and estimated completion dates.

OVERALL POSITION

We appreciate the Office of Inspector General (OIG)'s attention to the security categorization of
OLEM's electronic manifest system (e-Manifest). OLEM agrees with the importance of assuring
a level of security protection for e-Manifest that is commensurate with the level of risk posed by
the data contained in the system. The OIG's focus in this area has helped to increase our
understanding of the data to be housed in our system and the extent of risk posed by a potential
breach of e-Manifest's existing security controls.

Upon receiving the OIG's Management Alert on June 21, 2018, OLEM immediately initiated a
re-consideration of relevant factors related to e-Manifest's information sensitivity rating, as
advised by OIG in its Management Alert. We moved quickly to provide you an interim response
on June 29, 2018. In this response, we outlined several relevant factors for consideration[1] and, as

---

[1] The five initial factors that were considered include: (1) EPA completed prior coordination with DHS in 2017
ahead of e-Manifest launch; (2) Information on chemicals are already publicly available in other forums; (3) EPA
completed the Authority to Operate information security process in May 2018; (4) EPA has implemented moderate

further precaution, also instituted a temporary step to hold manifests containing certain wastes of concern outside of the electronic system. Our notes from the exit conference with the OIG on July 9, 2018, are that the OIG did not intend to imply action was needed to address the Management Alert in the days before launch.

Since issuing our interim response and in response to the OIG's Recommendation 1, OLEM has reengaged with the Department of Homeland Security (DHS) to again consider and evaluate the risks associated with the 56 specific P- or U-listed hazardous wastes that overlap with the DHS Chemicals of Interest list. Additionally, OLEM has explored further the nature and extent of information on these specific wastes that would be contained in the e-Manifest system. Specifically, in addition to the five relevant factors shared with you on June 29, 2018, OLEM now adds two additional relevant factors here:

Relevant Factor 6 – Significant Differences Between e-Manifest and DHS' CSAT System

Through our re-engagement with DHS's Information Security Compliance Division (ISCD), we have learned more about their system for storing information on chemicals of interest (COI) including important differences between that system and e-Manifest.

DHS collects information through the Chemical Security Assessment Tool (CSAT). Industry users use this tool to submit data to allow DHS to identify and regulate the security of high-risk chemical facilities using a risk-based approach. First, DHS' CSAT collects information on facilities that possess any of the approximately 350 chemicals of interest listed on Appendix A in 6 CFR part 27, which includes chemicals produced, stored, and used in commerce as designated by a Chemical Abstract Number (CAS). This information includes facility attributes, chemicals of interest, chemical quantities and concentrations, chemical locations, and whether the chemicals of interest are shipped off-site. In addition, CSAT collects information on types of chemical storage, physical states, process/storage temperatures, process/storage pressures, flow rates, and location types (e.g., in a building, above grade, below grade, or underground). Lastly, CSAT also contains information that is personally identifiable information (PII) and chemical vulnerability information (CVI). Based on the data stored and the nature of the information, CSAT is designated as a moderate-level system.

In contrast, the nature of information in e-Manifest is different than DHS' CSAT system in three important ways. First, unlike CSAT, e-Manifest does not include information on any chemical used in commerce, but only collects information on *waste* chemicals. Waste chemicals include chemicals that are off-specification, container residues, and spill residues, but which hold no reuse or reclamation value (reclaimed/reused commercial chemical products are not subject to RCRA regulation, including the manifest). Additionally, many waste streams contain derivatives or mixtures of the commercial chemical product, such as incinerator ash or wastewater treatment sludge. The result of this is that waste chemicals reported in e-Manifest oftentimes bear no resemblance to the pure chemical form and thus the system itself bears no resemblance to a chemical

level security controls beyond the security categorization; and (5) There is limited access to data within the system through role-based user accounts.

inventory. In other words, the purest forms of P and U wastes, those going to reclamation, are generally not part of the manifest system; moreover, P and U wastes at waste generation, treatment and disposal sites generally do not resemble an inventory of chemicals but instead are waste-like in their form and content. Second, e-Manifest contains a vastly reduced sub-set of the information compared to the DHS' CSAT, including no information on processing and handling of chemicals by chemical facilities. Lastly, unlike DHS' CSAT, e-Manifest does not contain PII or CVI (and also does not contain confidential business information (CBI)). These important differences could impact the categorization and account for the difference in security level between the two systems.

Relevant Factor 7 – Data Show Actual Hazardous Waste Quantities and Number of Handlers Above DHS Thresholds to be Small

To assess the risk of impact related to a breach of the e-Manifest system, OLEM conducted an analysis using data from its 2015 Biennial Report (BR) data[2] to understand further the nature of RCRA hazardous wastes and their relationship to COI. To do this, OLEM pulled reports of generators and receiving facilities that reported handling quantities of any of the 56 P- and U- listed hazardous wastes that overlap with COI.

Of the 56 P- and U- listed hazardous wastes that overlap with COI, OLEM, even with conservative assumptions, found only 13 wastes are handled by at least one facility exceeding the Release or Theft Screening Threshold Quantity (STQ) specified by the DHS over a 90-day period.[3,4]

Of these 13 wastes, only 68 handlers report quantities that could be above the DHS STQ. Out of the estimated 200,000 facilities that will eventually be in e-Manifest, these 68 represent three hundredths of a percent (.03%) of the total e-Manifest universe. This aligns with our understanding from the Environmental Technology Council that RCRA-permitted commercial waste management facilities have undergone DHS chemical security assessment, Top-screen reviews, and on-site inspections and have uniformly received low risk determinations.

Based on the two relevant factors here, and those previously presented, OLEM finds, at this point, that any impact to Agency operations, assets, or individuals or to the public from a

---

[2] The BR requires large quantity generators and TSDFs to submit every other year an annual report regarding the nature, quantity and disposition of hazardous waste generated and managed at their facility.

[3] RCRA large quantity generators cannot accumulate wastes for more than 90 days without a permit. Since the BR lists quantities as annual totals, OLEM's methodology was to take the annual total and divide by four (i.e., four 90-day periods a year) to estimate quantities of wastes onsite at any given time. (OLEM views this as a conservative estimate, considering that generators may ship more than four times a year, which would further reduce the quantity of waste on-site at any one time.) Similarly, OLEM assumes that TSDFs manage their waste within 90 days of receipt, rather than accumulating wastes over a full year. Finally, OLEM excluded mixture and derived from wastes from this analysis because of their highly diluted and waste-like attributes.

[4] DHS does not list specific threshold quantities for "Sabotage" threats and rather defers to "At Placarded Amount" or APA STQ. APA STQs depend on the material, its hazard class and packaging, and whether the chemical is shipped as bulk or non-bulk. In the absence of a clear threshold quantity for "Sabotage," OLEM instead relied on the other threshold quantities listed for "Theft" and "Release," where available.

potential breach to e-Manifest security controls would be limited and does not rise to the level of posing serious adverse impacts. OLEM has determined, based on our review and pending any new information or changes, that the e-Manifest system is appropriately categorized as a low-level system commensurate with the harm that could be caused if the e-Manifest system is compromised. OLEM will allow the system to accept all manifests while still indefinitely withholding from public disclosure certain manifest information related to the 56 hazardous wastes that overlap with COI, which is the same approach agreed to by DHS in 2017.

OLEM continues to agree with the OIG's recommendations in its Management Alert and, as such, commits to re-evaluating the security categorization annually or when there are significant changes or new information.

RESPONSE TO REPORT RECOMMENDATIONS

OLEM agrees with the OIG recommendations and provides corrective actions and estimated completion dates for each recommendation in the table below.

No.	Recommendation	Corrective Action(s)	Estimated Completion by Quarter and FY
1	Obtain an understanding of the impact of a breach of the EPA's Electronic Manifest system's hazardous material information from the U.S. Department of Homeland Security and re-evaluate the security categorization accordingly.	OLEM engaged with the U.S. Department of Homeland Security to factor DHS concerns into assessing the impact of a breach of the EPA's Electronic Manifest system's hazardous waste information and determined whether re-evaluation of the security categorization, independent of the annual re-evaluation, is necessary.	Completed as of the signature date of this memo.
2	In coordination with the EPA Office of Environmental Information and the National Institute of Standards and Technology, determine whether the Electronic Manifest system's hazardous material information should be handled as Pollution Prevention and Control Information or Inventory Control Information with special considerations for hazardous materials, and re-evaluate the security categorization accordingly.	OLEM will coordinate with the EPA Office of Environmental Information and, as necessary, the National Institute of Standards and Technology to determine whether the Electronic Manifest system's hazardous waste information should be handled as Pollution Prevention and Control Information or Inventory Control Information with special considerations for hazardous wastes, and determine whether re-evaluation of the security categorization, independent of the annual re-evaluation, is necessary.	2nd Quarter FY2019
3	Re-evaluate the security categorization of the	OLEM's e-Manifest Security Plan includes a process for re-	Completed May 17, 2018

	Electronic Manifest system annually or when there are significant changes to the system (including allowing the system to be used by emergency responders) as required by the EPA's Information Security – Risk Assessment Procedures.	evaluating the security categorization of the Electronic Manifest system annually or when there arc significant changes (including any potential use of the system by emergency responders) as required by the EPA's Information Security – Risk Assessment Procedures.	