November 29, 2018

TO: Dr. Mitchell Zais
Deputy Secretary

FROM: Aaron R. Jordan /s/
Assistant Inspector General for Investigations

SUBJECT: Re-Issue of Final Management Information Report, *Unauthorized Release of Non-Public Information* (ED-OIG/X42S0001)

That attached management information report originally issued on March 29, 2018, was reissued on November 29, 2018 to remove a statement on compliance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation. Although this is a reissuance of an existing report, the change cited does not impact any of the findings and suggestions contained. Because the reissuance does not impact the factual content of the management information report, March 29, 2018, will remain as the official issue date and does not affect the Office of Inspector General's Semiannual Report to Congress reporting requirements.

Beginning in July 2018, the U.S. Department of Education (ED) Office of Inspector General (OIG) underwent an external peer review to evaluate compliance with the Council of Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation (Blue Book). The peer review team concluded that the above listed MIR did not fully comply with the Blue Book in the following areas: Quality Control, Planning, and Data Collection.

In response to the peer review, ED OIG performed a quality assurance review of the MIR to determine whether its observations, conclusions, and suggestions were appropriate. The work included an evaluation of whether all statements in the final report were supported by sufficiently reliable and valid information. The review found nothing to question the accuracy of the observations, conclusions, and suggestions in the report – beyond the inclusion of the statement of compliance with Quality Standards for Inspection and Evaluation.

March 29, 2018

TO: Kent Talbert
Senior Policy Advisor, Delegated to Perform the Duties of the Deputy Secretary
Office of the Deputy Secretary

FROM: Aaron R. Jordan /s/
Assistant Inspector General for Investigations

SUBJECT: Final Management Information Report
Unauthorized Release of Non-Public Information
Control No. ED-OIG/X42S0001 (P17MAR30122)

The purpose of this management information report is to provide the U.S. Department of Education (Department) with suggested actions that could enhance the Department's ability to: (1) protect against the unauthorized release of non-public information, and (2) take appropriate administrative actions when an unauthorized release occurs. The OIG provided a draft of this report to the Department on January 4, 2018. The Department did not provide a formal response to the suggestions documented in this report.

Background

As part of the Office of Inspector General's (OIG's) mission to promote the integrity of the Department's programs and operations, the OIG investigates prosecutable violations of law by Department employees within the scope of their employment. Generally, due to limited resources, the OIG focuses its investigative efforts on Federal felonies. The OIG may also conduct non-criminal investigations of serious misconduct by Department employees. Two key factors that influence the decision of the OIG to investigate a matter are the likelihood a violation of law or policy can be proven and that substantive action can and will be taken.

Between May and October 2017, the Department requested that the OIG investigate three incidents in which there appeared to be unauthorized releases of non-public information.

May 17 and 18, 2017: the *Washington Post* published news articles that included information from the President's FY 2018 Budget Request for the Department. This information was not scheduled to be released until May 23, 2017.

June 20, 2017: *Politico* published an article indicating the Department's intention to delay the effective date of the borrower defense regulations published the prior November. The article stated that *Politico* had obtained internal documents showing "that the Trump administration

wrestled with the precise rationale for delaying the rules" and that the Department had "considered writing a new 'interim final rule' that pushed back the effective date of the rules by two years to July 2019."

October 31, 2017: we received notification from the Department regarding the unauthorized release of the draft document titled, *Assistance to States for the Education of Children with Disabilities: Preschool Grants for Children (NPRM)*. We were informed that the document was still in the clearance process and was still under deliberation and internal review when it became public.

In June 2012, the OIG issued an audit report titled, *Department's Negotiated Rulemaking Process for Gainful Employment* (ED-OIG/A19L0002). The report concluded that the negotiated rulemaking process should have specific documented protocols to protect sensitive information during the process. Specifically, the report stated that a lack of written protocols increases the risk to the Department that sensitive information may be inappropriately shared with parties who are not privileged to such information. During the audit, Department officials stated that everyone involved knew the sensitivity of the gainful employment regulations and that it was understood that sensitive information should not be shared with unauthorized personnel.

Observations

An OIG limited review revealed little Department policy or guidance in place regarding the unauthorized disclosure of Department documents to external sources, with the exception of the disclosure of personally identifiable information, proprietary information from companies, and security information. Administrative Communications System (ACS) Departmental Handbook OCIO-15, *Handbook for Protection of Sensitive But Unclassified Information* (Handbook), defines "Sensitive But Unclassified" (SBU) information and briefly discusses marking and labeling information, but the Handbook primarily focuses on security controls for information technology systems, is over a decade old, and is not updated to be consistent with current Federal regulations (see 32 Code of Federal Regulations (C.F.R.) Part 2002, *Controlled Unclassified Information*). Of the three incidents reported to the OIG, only the May release of budget information falls within one of the approved controlled unclassified information (CUI) categories and could also meet the Department's definition of SBU based on Office of Management and Budget Circular A-11, section 22.1. The other two incidents involved non-public information for which we found no regulation or policy specifically prohibiting their disclosure.

Handbook OCIO-15, section 1.6 provides that "the gross negligence or willful disclosure of **sensitive but unclassified** information may result in disciplinary action, including but not limited to, removal from employment" [emphasis added]. The Department's Table of Penalties for Stated Offenses, Human Capital Policy (HCP) 751-1, *Discipline and Adverse Actions*, Exhibit 2, lists these possibly relevant offenses: "32. Failure to safe-guard confidential materials," and "33. [M]isuse or unauthorized use of Government…information." Only the budget information met the definition of SBU, but it was not properly marked. The Table of Penalties describes no offense that clearly addresses the release of non-public information that is not SBU or CUI.

Challenges

While evaluating the three incidents of alleged unauthorized releases of non-public information, we identified challenges to criminal prosecution or taking significant administrative actions against individuals responsible for the release of this type of information.

Although the aforementioned incidents are examples of possible unauthorized releases of non-public information by Department employees, unlike classified information, personally identifiable information, or proprietary information, we were unable to find specific protections in criminal law for the information released in these incidents. Thus, it is unlikely that the OIG could obtain a Federal prosecution for general releases of non-public information.

The Department can take administrative action for employee misconduct, but officials from the Department's Office of Human Resources, Workforce Relations Division (WRD) indicated that the clarity with which the employee was on notice concerning the prohibition against unauthorized disclosure or the sensitivity of the information could impact the Department's ability to successfully administer discipline. The WRD officials did state that the disclosures might be viewed as a violation of the Standards for Ethical Conduct for Employees of the Executive Branch (5 CFR § 2635.703). The WRD officials, after consultation with the Office of Legislative and Congressional Affairs, also indicated there is no specific policy addressing the disclosure of work-related non-public information to the media. The absence of specific Department policy and the lack of markings on the document to provide notice to employees would be mitigating factors that could potentially lessen the administrative remedies available to the Department for these or similar incidents.

Additionally, obtaining sufficient evidence to identify the responsible people and prove that they "leaked" information is difficult, even in classified environments where controls are more stringent. As documents are circulated among increasingly larger groups of individuals, the challenges continue to increase, particularly if some of the individuals involved do not work at the Department.

Suggestions

The following are suggested actions for the Department to consider regarding the prohibition on releasing non-public information and enhancing management controls.

1. Develop interim policy requiring Department employees to clearly mark non-public documents with markings that indicate the information is not for public release.

2. Provide training to all Department employees and at least once again every two years thereafter on the proper protection and marking of controlled unclassified information, as specified in 32 C.F.R. § 2002.30.

3. Create a new ACS Directive to address prohibitions on the unauthorized release of sensitive or non-public information, the definition of controlled unclassified

information, and proper marking of documents as indicated in Executive Order 13556, 32 C.F.R. Part 2002, and the guidance located at https://www.archives.gov/cui.[1]

4. Update ACS Handbook OCIO-15, as necessary, for consistency with the new ACS Directive and pertinent National Institute of Standards and Technology publications.

5. Evaluate the current list of offenses within the table of penalties located in HCP 751-1, and consider the inclusion of "Unauthorized Release of Non-Public Information" and/or "Unauthorized Release of Controlled Unclassified Information."

6. Apply Information Rights Management (IRM) to sensitive electronic documents during the review process when additional security controls are warranted. IRM can be used to prevent a document from being opened, forwarded, copied, or printed, except by those who have permissions to do so.[2]

Department Response

The Department did not provide a formal response to the suggestions documented in this report.

Conclusion

Implementing the provided suggestions could assist the Department in protecting against the unauthorized release of non-public information and with taking appropriate administrative action when allegations are substantiated. It may also increase the potential for the OIG to obtain a criminal prosecution in certain cases. The decision by the OIG to investigate a future "leak" allegation will be based upon the specific facts of that situation. These facts include, but are not limited to, the nature of information that was leaked, the ability to identify all personnel who had access to the released information and number of personnel, the impact of the release on the Department and/or the Government generally, the markings applied to any documents, and whether the information could have been released through a Freedom of Information Act request.

Administrative Matters

This Management Information Report (MIR) issued by the Office of Inspector General will be made available to members of the press and general public to the extent information contained in the report is not subject to exemptions in the Freedom of Information Act (5 U.S.C. § 552) or protection under the Privacy Act (5 U.S.C. § 552a).

---

[1] There may be times when what may be viewed as a "leak" or an unauthorized release of non-public information could involve a protected disclosure by a Department employee. Therefore, the policy and handbook referred to in 3 and 4 above should take into consideration whistleblower rights and protections.

[2] The Department's IRM capabilities can be applied within Microsoft products (such as Word and Outlook) as long as all of the personnel who need to review a document have Department network accounts. If a document must also be read by individuals outside of the Department, Digital Rights Management within Max.gov may be used, which will require each reviewer to have a Max.gov account.

If you have any questions, please contact Mark A. Smith, Deputy Assistant Inspector General for Investigations, at (202) 245-7019.

Attachment
Methodology

cc: Office of the General Counsel

Methodology

The OIG reviewed the information provided it concerning the alleged unauthorized releases of non-public information between May and October 2017. On November 7, 2017, after identifying common challenges to criminal prosecution or administrative action for the incidents reviewed, the OIG decided to conduct a limited review to determine potential steps the Department could take to protect against the release of non-public information and to strengthen the potential for action when an unauthorized release occurred.

As part of our initial review of the allegations, the OIG searched the U.S. criminal code and consulted with an Assistant United States Attorney to identify potential criminal statutes that may have been violated and assessed the likelihood of a criminal prosecution. The OIG also did a search for and conducted a limited review of relevant policies and guidance on ConnectED, the Department's intranet. Additionally, the OIG consulted with WRD officials to determine if there were violations of policy and assessed the likelihood of significant administrative action against responsible individuals.

To conduct our review for this MIR, the OIG synthesized its previous work and conducted a limited review of Federal regulations concerning the protection of unclassified information. We also did a limited review of technical solutions currently available to the Department. Based on this work, the OIG developed suggested actions for the Department's consideration.

The OIG provided a draft of this report to the Department on January 4, 2018. The Department did not provide a formal response to the suggestions documented in this report.

The OIG conducted its review from May 2017 through December 2017 in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Investigations.