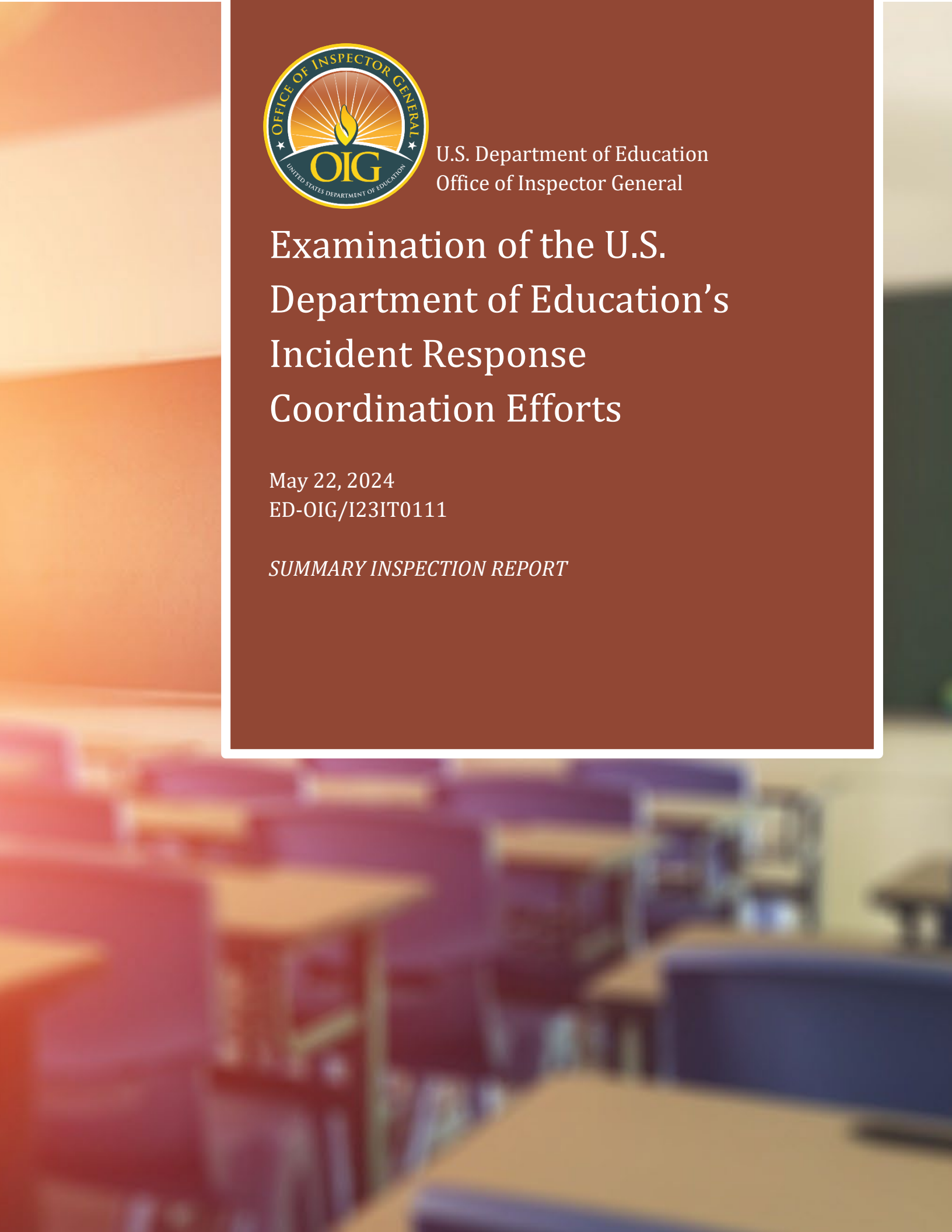

U.S. Department of Education
Office of Inspector General

Examination of the U.S. Department of Education's Incident Response Coordination Efforts

May 22, 2024
ED-OIG/I23IT0111

SUMMARY INSPECTION REPORT

May 22, 2024

TO: Dennis Johnson
Acting Chief Information Officer

FROM: Kevin J. Young /s/
Assistant Inspector General
Technology Services
Office of Inspector General

SUBJECT: Summary Final Inspection Report, "Examination of the U.S. Department of Education's Incident Response Coordination Efforts," Control Number ED-OIG/I23IT0111

Attached is the Summary Final Inspection Report of "Examination of the U.S. Department of Education's Incident Response Coordination Efforts," Control Number ED-OIG/I23IT0111 for public view. Given the sensitivity of the information it contains, the full report is restricted.

Summary of Report Results

What We Did

The objective of our inspection was to determine if the U.S. Department of Education (Department) has established and implemented controls throughout all phases of its incident response lifecycle to ensure compliance with Federal guidance and regulations. To accomplish our objective, we interviewed Office of Chief Information Officer and Federal Student Aid officials, reviewed documentation, and performed limited testing related to the incident response program and operations. Specifically, we reviewed and assessed incident response policies, procedures, guidelines, and checklists used by the Department and contractors; tested incidents reported to the Department during the period covered by the inspection to assess its compliance with policies and Federal requirements; and reviewed the Department's information technology contract requirements and inspected a sample of incident response program contracts to assess compliance with policies, Federal guidance, and regulations.

What We Found

Although the Department established policies, procedures, and guidance governing its incident response program, we noted areas where it can improve its current process. Specifically, the Department did not (1) consistently follow Federal mandates or Departmentwide policies governing cyber attribution, (2) consistently include required documentation for all incidents, (3) ensure data loss prevention was properly configured, and (4) ensure data loss prevention incidents were closed based on adequate justification.

What We Recommend

We identified 6 conditions and made 12 recommendations to improve the Department's incident response program. In addition, we identified observations related to information technology contract inventory and the oversight and enforcement of Department security requirements, which were presented in the Other Matters section of the full report.

Department Comments

We provided a draft of this report to the Department for comments. The Department provided a response letter that included technical comments that we considered and addressed, as appropriate. Of the 12 recommendations made, the Department agreed with 4 of them, partially concurred with 4 of them, and did not concur with 4 of them (although subsequent actions taken met the intent of 2 of them).