FOR IMMEDIATE RELEASE
July 7, 2022

DOJ OIG Releases Report on DOJ's Cyber Supply Chain Risk Management Efforts

Department of Justice (DOJ) Inspector General Michael E. Horowitz announced today the release of a report examining the Department's cyber supply chain risk management (C-SCRM) efforts. C-SCRM is the process for managing exposure to cybersecurity risks throughout the supply chain and for developing response strategies, policies, processes, and procedures to combat those risks. Ineffective management of C-SCRM increases the risk of introducing products or services into DOJ's information technology (IT) environment that could compromise the integrity of its systems and data. DOJ operates two distinct C-SCRM programs—one by and focused on the Federal Bureau of Investigation (FBI); and a second operated by the Justice Management Division (JMD) that is focused on all non-FBI Department components.

The DOJ Office of the Inspector General (OIG) found several areas for improvement in DOJ's C-SCRM efforts, including:

- **JMD Lacked Resources to Effectively Manage its C-SCRM Program.** Overall, JMD lacked the personnel resources to effectively manage its C-SCRM program, resulting in widespread noncompliance, outdated guidance, inadequate threat assessments, and insufficient mitigation and monitoring actions. JMD relies on Department components to independently meet the C-SCRM requirements and to develop procedures and internal controls to implement them on their own. We assessed C-SCRM compliance by several of the largest non-FBI DOJ components and found that only the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Drug Enforcement Administration (DEA) were compliant with the JMD C-SCRM requirements. We concluded that JMD needed to provide communication, outreach, and training to Department components and develop procedures to periodically assess their efforts; or C SCRM controls could be bypassed and high-risk IT could be installed without JMD authorization or a risk mitigation plan.

- **The FBI Can Improve Elements of its C-SCRM Program.** While the FBI's C-SCRM program was more modern than JMD's, it was also in need of improvement. We found that hundreds of millions of dollars in IT-related goods and classified services may have improperly bypassed the FBI's C SCRM process, due in part to FBI procurement officials' misunderstanding or unawareness of the C-SCRM requirements. Purchases that improperly bypass the C SCRM process may not receive mitigation steps to address the identified risks, thereby increasing supply chain risk throughout the FBI. Additionally, the FBI needed to improve its key deliverables to better align with Intelligence Community requirements, enhance both its risk mitigation and continuous monitoring efforts, and better integrate C-SCRM across the organization.

- **The DEA Should Develop a C-SCRM Program, as Required by an Intelligence Community Directive.** We determined that the DEA's Office of National Security Intelligence, a member of the U.S. Intelligence Community, had not established a supply chain risk management program as required by an Intelligence Community directive.

- **Other JMD and FBI Noncompliance and Areas of Improvement.** Both JMD and the FBI needed to comply with congressional and external C SCRM requirements and improve their information sharing efforts within the Department as well as with the U.S. Intelligence Community.

The DOJ OIG made a total of 17 recommendations, specifically to JMD, the FBI, and the DEA to assist the Department in improving its organizational approach to C-SCRM. These Department components agreed with all the recommendations.

Report: Today's report can be found on the OIG's website at the following link: https://oig.justice.gov/reports/audit-departments-cyber-supply-chain-risk-management-efforts

###