ANNOUNCEMENTS

Prohibited Disclosure of Unclassified, Sensitive Information Without Proper Authorization

October 20, 2023

Like classified national security information, all ATF employees have a duty to adequately protect and secure unclassified sensitive information. This announcement serves to remind all ATF employees that the unauthorized disclosure of sensitive but unclassified (SBU) information is strictly prohibited.

SBU is information that is **not** classified for national security reasons, **but** that warrants/ requires administrative control and protection from public or other unauthorized disclosure for other reasons. The loss or misuse of, or unauthorized access to, SBU information can adversely affect the agency's mission, the conduct of federal programs or the privacy to which individuals are entitled. SBU information may be designated in various ways, including but not limited to, "For Official Use Only" (FOUO), "Limited Official Use" (LOU), and "Law Enforcement Sensitive "(LES). SBU information may include investigative, proprietary, regulatory and tax information, as well as other sensitive information such as fiduciary and personally identifiable information (PII).

There have been multiple instances recently where employees have failed to adhere to unclassified sensitive information policies or procedures. Such failure may lead to disciplinary action, including suspension or removal from federal service. Additionally, the unauthorized taking or disclosure of certain classes of SBU information may lead to criminal charges. Within the past year, an ATF employee pleaded guilty and was criminally convicted in federal court of theft of government records related to SBU information. As a result, this employee is no longer with ATF. The impact of this employee's unauthorized disclosures directly affected ATF's mission and such actions will not be tolerated.

It is imperative that employees exercise good judgement and common sense when using, handling and storing SBU information. ATF and DOJ policies such as ATF Handbook 7250.1, Automated Information System Security Program (July 26, 2006), Rules of Behavior and Customer Agreement for Computing Devices (May 2, 2011), and DOJ

Memorandum: Safeguarding Sensitive and Other Forms of PII (Aug. 13, 2015), address the continuing obligations that employees have regarding SBU information.

Please direct any questions to Mark Riddle, Chief, Information Security Branch, at [redacted].