ELLEN F. ROSENBLUM
Attorney General

FREDERICK M. BOSS
Deputy Attorney General

DEPARTMENT OF JUSTICE
CRIMINAL JUSTICE DIVISION

MEMORANDUM

DATE: February 2, 2015

TO: INTEL SECTION WORK GROUP

FROM: MATT MCCAULEY, AAG

SUBJECT: Intelligence Systems Questions

As part of the process of reviewing DOJ's criminal intelligence systems for compliance with 28 CFR part 23 as well as Oregon law governing DOJ's criminal intelligence systems and operations I have researched several questions regarding our systems. My research lead me to have a discussion with John Wilson. John is an attorney who helped draft 28 CFR part 23 and who has trained on it's application for years. John's analysis of each question and answer as well as proposed solutions is as follows:

Questions:

1. Have we accidentally created a criminal intelligence system which falls under 28 CFR 23 rules? If so, what is your advice for dealing with it? If not, why not and what is your advice for a best practice in this situation?

Response: No, any criminal intelligence information (CII) received by Oregon DOJ (for this response, I will use CII disseminated by the WSIN intelligence project and received by Oregon DOJ) and its authorized CII components (such as the Oregon TITAN fusion center, the Oregon HIDTA, etc.) that is retained in the Oregon/Oregon DOJ Microsoft Outlook system, if not being retained for the purpose of the "interagency exchange or dissemination" of the information, an essential requirement under the definition of a "criminal intelligence system" under 28 CFR § 23.3(b)(1), would not be considered a "criminal intelligence system."

However, CII received from WSIN that is subject to 28 CFR Part 23 would be subject to the requirement of 28 CFR § 23.20(e) that: "A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity." While the information may be retained by Oregon DOJ for internal proposes, such as analysis, audit, or to meet state information retention requirements, any further dissemination outside Oregon DOJ would be subject to: (1) WSIN third party dissemination requirements or, at a minimum, 28 CFR § 23.20(e); and (2) any other procedures regarding CII receipt, maintenance, security, and dissemination

established by WSIN that are consistent with the operating principles of 28 CFR Part 23 (28 CFR §23.20 (f)(1), including use of "technologically advanced computer software and hardware designs to prevent unauthorized access to the system" (28 CFR § 23.20 (g)(1)) and storage of information "in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization" (28 CFR § 23.20 (g)(3)).

Use of encryption or secure networks is advised for the exchange of any law enforcement sensitive information. Also, IS/IT personnel who have access to CII and other law enforcement sensitive information may be required to sign a nondisclosure agreement and/or required to participate in appropriate training.

My understanding from this information is that the Outlook data itself is not a criminal intelligence system but the intel on it requires that we take steps which we have already contemplated including having the CIU use WISN and HISN email as much as possible and having DOJ IT personnel sign documents of non-disclosure.

2. Why is criminal investigative information not criminal intelligence?

Response: Only criminal intelligence records that meet the reasonable suspicion criteria and other 28 CFR Part 23 operating principles and are shared between agencies by an intelligence project are subject to the regulation. Fact-based or uncorroborated information (including information in case investigative files, case management systems, incident/offense reports, field interview cards or contact files, criminal history records, arrest blotters, RMS data, tips and leads, SARs, etc.) and other types of information or intelligence gathered/collected and shared by SLTT law enforcement and intelligence agencies that are not premised on a determination of reasonable suspicion are not subject to 28 CFR Part 23.
An investigator, for example, might start the process of developing a criminal case using the information contained in a tips and leads file. Investigating the tips and leads information could produce sufficient information to conduct a criminal investigation. Additional fact gathering may result in obtaining a body of information that, when analyzed (evaluated), is determined to meet the reasonable suspicion standard. If it meets the reasonable suspicion standard, a record on that subject could be entered into a criminal intelligence database. The information from the tips and leads file, as well as any other investigative information gathered and retained in an investigative file, would need to be kept as supporting documentation for that record and retained, stored, and used in accordance with the investigative agency's policies and procedures.