Deputy Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

October 18, 2016

Policy Directive 045-04

MEMORANDUM FOR: Department Component Heads

FROM: Alejandro N. Mayorkas
Deputy Secretary

SUBJECT: **Department Policy Regarding Investigative Data and Event Deconfliction**

This memorandum sets forth the Department of Homeland Security (DHS) policy for investigative data and event deconfliction and the use of related deconfliction systems in the course of certain law enforcement activity. This policy requires, first, that DHS law enforcement Components conduct investigative data and event deconfliction during the course of criminal investigations, to more effectively coordinate investigative activity and ensure officer safety. Second, recognizing that the routine use of event deconfliction systems can also have a positive impact on officer safety during the course of non-investigative DHS law enforcement activity, this policy strongly encourages DHS law enforcement Components to integrate, as appropriate, the use of event deconfliction for significant DHS law enforcement operations.

Background, Purpose, and Definitions

The law enforcement community generally defines "deconfliction" as the sharing of limited investigative information among federal, state, local, and tribal law enforcement entities in order to identify common interest or activity. For the sake of clarity in its application, this policy refers to such deconfliction, in the general sense, as "investigative deconfliction."

For purposes of this policy, investigative deconfliction consists of the following categories:

- *Investigative Data Deconfliction*[1]: the sharing of significant investigative information in order to identify common investigative interest or activity among criminal investigators.[2] Significant investigative information includes, but is not limited to, information that pertains to the target or subject of an open investigation (including name, date of birth, and gender); addresses; airplane tail numbers; Blackberry PINs; Bureau of Prisons IDs; e-mail addresses; Internet Protocol addresses; Uniform Resource Locator address (often referred to as the "website" or "web address"); financial account numbers (including virtual currency user/account identifiers); International Mobile Equipment Identity numbers; license plate numbers; telephone numbers; push-to-talk IDs; social network IDs (including dark net and Onion Router IDs); state/local prisoner IDs; and, Vehicle Identification Numbers.

- *Event Deconfliction*: the sharing of significant investigative information that relates to significant or anticipated operations in order to determine whether law enforcement personnel are conducting an event in close promixity to one another at the same time. This information includes, but is not limited to, undercover operations; surveillance; executing search warrants or arrest warrants; buy-busts; controlled deliveries; and other related criminal investigative enforcement operations.

Currently, there are numerous means by which DHS law enforcement personnel and other law enforcement agencies nationwide conduct deconfliction. This policy focuses on five such methods: (1) the Deconfliction and Information Coordination Endeavor (DICE); (2) the Regional Information Sharing Systems (RISS) Officer Safety Event Deconfliction System (RISSafe); (3) the Secure Automated Fast Event Tracking Network (SAFETNet); (4) Case Explorer; and, (5) the Export Enforcement Coordination Center (E2C2).

The DICE system is an Internet-based, Department of Justice (DOJ)-owned application that provides participating federal, state, local, and tribal law enforcement agencies with the ability to identify data related to common investigative interests or activity. Once DICE identifies a common piece of investigative data, typically referred to as a conflict or investigative overlap, the system immediately notifies relevant law enforcement personnel of the match and provides contact information for the owner(s) of the records, but does not give access to the matched investigative data itself. This enables law enforcement personnel to deconflict, share information, and coordinate efforts while protecting the integrity of ongoing investigations. DICE currently permits deconfliction of more than one dozen data points, although this number may continue to

[1] While some in the law enforcement community draw a distinction between "investigative data deconfliction" and "target deconfliction," these two categories are combined for purposes of this policy.
[2] *Significant investigative information* is defined, for purposes of this policy, as relevant and noteworthy information developed or identified through an open criminal investigation.

grow in order to meet the needs of participating entities. Additional information about DICE, including directions for obtaining a DICE user account, may be found on DOJ's DICE website (https://dice.usdoj.gov).

RISSafe, SAFETNet, and Case Explorer are three primary regional event deconfliction systems. These Internet-based systems enable law enforcement personnel to identify potential operational conflicts in the field. When certain elements (such as time, date, and location) are matched between two or more upcoming events or operations, the affected agencies or personnel are notified of the conflict. Law enforcement agencies across the United States use these systems to conduct domestic deconfliction and are valuable tools to promote officer safety.

RISSafe, SAFETNet, and Case Explorer have been integrated so that entering an event into one system deconflicts against all three. Further, many longstanding local event deconfliction mechanisms used by DHS law enforcement Components interface with these systems. Law enforcement personnel can obtain access to RISSafe, SAFETNet, and Case Explorer through, respectively, the appropriate RISS Center, High Intensity Drug Trafficking Area (HIDTA) Investigative Support Center, and the Washington/Baltimore HIDTA.

E2C2 was created pursuant to Executive Order 13558, dated November 9, 2010, to coordinate export control enforcement activities and investigations and to minimize enforcement conflicts among executive departments and agencies. DHS law enforcement Components conducting export enforcement activities and investigations, including counter proliferation, already deconflict investigative data through E2C2.

Several DHS law enforcement Components have in place a variety of investigative deconfliction policies, procedures, and practices, using various investigative deconfliction systems and mechanisms. These include, to varying degrees, the systems described above. However, the Department can benefit from a more unified policy governing investigative deconfliction activities.

Policy

Investigative Deconfliction

Through implementation of this policy, the Department will achieve more consistent and effective investigative deconfliction policy and practice. This, in turn, will help to identify links between ongoing criminal investigations, facilitate greater law enforcement collaboration and coordination, avoid conflicting equities, and promote officer safety.

This policy requires that DHS law enforcement Components, in the course of criminal investigations, conduct investigative data deconfliction and event deconfliction as described above. At a minimum, the DHS law enforcement components must:

- conduct investigative data deconfliction through DICE or, in the case of export enforcement activities and investigations (including counter-proliferation), E2C2,[3] and

- conduct domestic event deconfliction through the appropriate regional event deconfliction system, namely RISSafe, SAFETNet, or Case Explorer.[4]

DHS law enforcement Components should be aware that some information may be classified at a higher level than the classifications of the systems listed in this policy. Consequently, that particular information is not captured for deconfliction purposes in these systems. Similarly, some information may be so sensitive that even limited sharing poses a serious threat to the integrity of an investigation. For example, national security investigations and certain non-routine criminal investigations, such as particularly sensitive cases involving corruption of law enforcement officers, may require special handling that renders deconfliction, at least temporarily, imprudent. However, such circumstances should be the exception to this policy and must recieve supervisory review and approval.

Within 90 days of the issuance of this policy, each DHS law enforcement Component that conducts criminal investigations will issue implementing guidance consistent with this policy to all affected personnel. Components will coordinate their respective policies with DHS Law Enforcement Policy.

To the extent that affected law enforcement Components determine, following an appropriate review, that existing deconfliction policies, procedures, and practices are consistent with this policy, these may be retained in lieu of newly-issued policies, practices and procedures. Nothing in this policy prohibits continued investigative deconfliction through additional systems or mechanisms not specifically mentioned here.

Other Law Enforcement Event Deconfliction

DHS recognizes that making event deconfliction a routine practice for all law enforcement personnel engaged in law enforcement actions or activity, not solely those conducting criminal investigations, is important to ensuring officer safety and avoiding "blue-on-blue" events. By virtue of DHS's complex mission and broad authorities, DHS

[3] Use of an investigative data deconfliction system that interoperates with DICE satisfies this requirement.
[4] Use of an event deconfliction system that interfaces with one of these three systems satisfies this requirement.

law enforcement personnel routinely plan and execute operations in the field. For example, as a result of their enforcement responsibilities, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, United States Secret Service, United States Coast Guard Investigative Service, and Federal Protective Service officers and agents regularly apprehend and arrest convicted criminals, fugitives, and others who pose a threat to public safety.

This policy strongly encourages DHS law enforcement Components to integrate domestic event deconfliction into all relevant DHS law enforcement operations using RISSafe, SAFETNet, or Case Explorer, regardless of whether the relevant law enforcement activity involves a criminal investigation. Use of these regional event deconfliction systems will enable DHS law enforcement personnel to identify operational conflicts, collaborate with other law enforcement agencies, and leverage law enforcement event information to more effectively and safely carry out the law enforcement mission.

DHS also recognizes that there are and will continue to be various inter- and intra-agency efforts to enhance the information technology systems that support investigative data and event deconfliction processes. Such advances are both expected and encouraged. As deconfliction mechanisms improve and evolve, there may be a need to revisit specific elements of this Policy Statement to reflect these developments.

All questions regarding the scope and implementation of this policy should be directed to the Deputy Assistant Secretary for Law Enforcement Policy, Office of Policy.