



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 11, 2014

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Randall C. Coleman, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, before the Committee on May 13, 2014, at a hearing entitled: "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?" We apologize for our delay in responding to this request.

Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Peter J. Kadzik
Assistant Attorney General

Enclosure

cc: The Honorable Charles E. Grassley
Ranking Member

Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the May 13, 2014, Hearing Before the
Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism
Regarding "Economic Espionage and Trade Secret Theft:
Are Our Laws Adequate for Today's Threats?"

Questions Posed by Senator Whitehouse

As we discussed, multiple units within the FBI are responsible for economic espionage and trade secret theft cases.

1. Please explain the division of responsibility for these cases within the Bureau, and specifically the roles of the Counterintelligence, Cyber, and Criminal Investigative Divisions.

Response:

Because the theft of trade secrets can involve a range of activities and circumstances, three programs in the FBI share the responsibility for investigating these violations. When the FBI learns of a possible trade secret theft, we assess the available information to determine whether the theft resulted from an insider or a cyber intrusion. If the theft resulted from a cyber intrusion and there is no insider nexus, the Cyber Division provides program management for the investigation. If the trade secret theft appears to be the work of an insider and there is a possible foreign nexus, the investigation is managed by our Counterintelligence Division; if theft by an insider does not appear to have a foreign nexus, it is managed by the Financial Institution Fraud Unit in the Criminal Investigative Division.

2. How and on what basis is the determination made as to where a case is assigned?

Response:

Please see the response to Question 1, above.

3. What efforts are made and what procedures are in place to ensure that agents in all relevant divisions are sharing information and communicating with each other on a regular basis?

These responses are current as of 6/20/14

Response:

The FBI is constantly working to ensure that information is shared across divisions and that resources are used efficiently. Strategic analysts are embedded in each operational division at FBI Headquarters. These analysts are led by an Intelligence Deputy Assistant Director (DAD) who reports to the FBI's Directorate of Intelligence (DI). To ensure the cross-programmatic sharing of information, the DI has developed a standardized framework for collecting, reporting, and disseminating intelligence. Within the operational divisions, threat-based fusion cells now serve as intelligence teams to integrate all aspects of the intelligence cycle, providing a more strategic and nimble approach to identifying and mitigating current and emerging threats and facilitating more seamless information sharing among Intelligence Analysts and Special Agents across programs. Each fusion cell reports to its program's Intelligence DAD, and these DADs meet monthly to ensure close collaboration.

4. Has the FBI considered consolidating responsibility for these cases within one unit, and for how long does the FBI think this will remain a sensible division of responsibilities?

Response:

The FBI's DI ensures that the intelligence elements embedded in our operational divisions communicate effectively in order to ensure a cross-programmatic approach to threats. As noted above, the theft of trade secrets can involve a range of activities and circumstances. The FBI believes the delineation of responsibilities discussed in response to Question 1 is the most effective use of our resources because it allows us to leverage the subject matter expertise offered by each program to address the particular activities and circumstances involved in a given case. As we have in the past, we will continue to evaluate our organizational structure and business processes to ensure we are best positioned to address the evolving threat.