Recommendation Guidance

Engaging with Federal Government Regulators and Officers on Export Controls and Sanctions Compliance Investigations

This Guidance provides general recommendations for dealing with federal government regulators and officers, focusing on export controls and sanctions compliance investigations, which can lead to administrative and criminal enforcement actions.

Background

In February 2023, approximately one (1) year after Russia's invasion of Ukraine and the imposition of massive export controls and sanctions the US Departments of Justice (DOJ) and Commerce, Bureau of Industry and Security (BIS), Office of Export Enforcement (OEE), along with the Federal Bureau of Investigation (FBI) and Homeland Security Investigations (HSI), launched the Disruptive Technology Strike Force. Since its formation, the Defense Department's Defense Criminal Investigative Service (DCIS) has become a partner agency. The Task Force is designed to protect supply chains and prevent advanced technologies from being unlawfully acquired by foreign adversaries, such as China, Russia, Iran, North Korea, and other state and non-state actors.

Although "disruptive technologies" is not defined, the Task Force is focused on technologies that the can pose a national security threat to the United States, such supercomputing, artificial intelligence (AI), advanced manufacturing equipment and materials, quantum computing, and biosciences.

Since its formation, the Task Force has coordinated with the DOJ's Task Force KleptoCapture, another interagency law enforcement task force that is dedicated to enforcing US export controls and sanctions that the US and its allies and partners have imposed in response to Russia's invasion of Ukraine.

Preparing for Engagement with Federal Government Regulators and Officers

Now, more than ever before, there is an increased risk that companies will be contacted by federal government regulators and law enforcement officers requesting documents and information regarding exports of goods, technologies, and software, and a company's

compliance policies and procedures. These requests can range from a BIS analyst sending an email request for documents regarding certain exports to Special Agents from DCIS, FBI, HSI, or OEE (or from any combination of these and other agencies) appearing in-person for an Outreach Visit, service of an administrative subpoena by an agency such as the Office of Foreign Assets Control (OFAC), to a grand jury subpoena issued from a federal court in connection with a criminal investigation.

In a worst case scenario, federal agents will execute a search warrant at the company, temporarily shutting down the business, imaging computers, servers, and other devices, removing valuable business equipment, documents, and personal devices, and performing a thorough search of the premises.

In such circumstances, a company's policy and response should be to carry out its obligations fully and fairly, while also understanding the extent of its obligations and being advised in connecting with carrying out its obligations while protecting its rights and interests to the greatest extent possible. If contacted by a federal agency for any reason (including an "Outreach" visit), if it is not obvious or expressly stated, ask the agents whether the contact is in connection with a civil or criminal investigation and, if so, contact counsel. And always be respectful and polite!

Having a written corporate compliance policy that incorporates guidance issued by government departments and agencies regarding export controls and sanctions is one facet of preparing for engagement by government regulators and law enforcement officers.

A compliance policy should be risk-based and relevant to the company's operations. For example, if a company's goods, technologies, and software are not subject to export controls under the International Traffic in Arms Regulations (ITAR), there is no reason for the ITAR to be addressed in its compliance policy. But if a company sells products through a network of global distributors, resellers, agents, and others, but fails to refer to in its compliance policy and obtaining end-use/ end-user statements or performing restricted party screening and other due diligence, questions will surely be raised in the event of an investigation.

In addition, it must be emphasized that all communications—written and oral, regardless of format and media—made to federal government officers must be truthful. Failing to be truthful with a federal agent can result in criminal (as well as administrative) charges being brought against the individual. It is better to say nothing than be misleading or uttering falsehoods. A company cannot tolerate inaccurate or false statements or omissions made by any owner, member, shareholder, director, officer, employee, or other company representative, to any federal government regulators or officers.

Clear instructions on who should be contacted in the event anyone associated with a company is contacted by federal government officers should also be conveyed to a company's workforce to ensure proper handling of the government's engagement.

Contacts by Government Agencies

Whatever the means or method, if a company is contacted by a federal government regulator or officer it is suggested that these actions be followed by the person contacted:

- ***Immediately notify the company's compliance or security officer(s), Legal Department, or outside legal counsel, as well as any others, as instructed by company policy and those persons who are immediately contacted.***

- The person contacted should not reply to any inquiry or request before without being directed to do so by the company's compliance or security officer(s), Legal Department, or outside legal counsel, and any others, as instructed by company policy.

- If an interview is requested, the person contacted should know that they have the right to decline an interview and provide no information.
  - If the person contacted decides to proceed with an interview, they should be made aware of their rights, including:
    - That they can request counsel to be present during the interview, possibly coordinated or provided by the company;
    - If the interview relates to a potential criminal violation, they should be made aware that anything stated can be used against them in a criminal proceeding, whether or not they receive a warning about this. A warning that anything said can be used against them is constitutionally required ***only*** for a person who is being taken into custody.
      - Note: If possible, before the interview occurs, it should be understood whether the person to be interviewed may make statements that are binding on the company.
    - Any statements that are provided must be truthful.

Document Requests, Subpoenas, and Search Warrants

A federal government officer seeking documents is likely to use one of three (3) methods: an informal request, by email, phone call, or in-person visit (scheduled or unscheduled); a subpoena (a legal command that requires the production of books, records, and other items identified in the subpoena); or a search warrant (an order issued by a judge that authorizes federal government officers to search for and seize any form of property that may be evidence of a crime, contraband, or the "fruits" of criminal activity.

Regardless of the method used, the company's policy should consider the following instructions:

- Immediately notify the company's compliance or security officer(s), Legal Department, or outside legal counsel and wait for further instructions before showing or providing any documents or items to the federal government officers.

- If the federal government officers request that the person **consent to a search** (or consent to imaging computers, laptops, and other devices), the person should DECLINE the request and the federal government officers should be referred to the company's compliance or security officer(s), Legal Department, or outside legal counsel.

- If the federal government officers have obtained a search warrant in connection with a criminal investigation, officers often appear in numbers in an effort to take control of the premises or portion of the area to be searched.
    - During the time that officers are executing the search warrant:
    - Follow the instructions of the compliance or security officer(s), Legal Department, and outside counsel;
    - Follow the officer's instructions;
    - To the extent practical, provide necessary cooperation in an effort to minimize disruption to the business operations;
    - Do nothing that actually or might be perceived as obstructing the execution of the search warrant; and
    - Minimize communications with the officers to acknowledge an understanding of their instructions and do not engage in conversations.
    - Always be respectful, polite, professional, and non-confrontational.

If officers request any interviews, please follow the above guidance.

This Recommendation Guidance is intended to provide general information for companies and interested individuals and is neither intended to be nor should it be relied on as specific legal advice regarding export controls and sanctions inquiries and investigations conducted by federal government regulators and officers.

Yormick Law LLC thanks Special Agent Glenn Karabeika, (Ret.) US Department of Homeland Security Investigations, of Strategic Investigations and Consulting, for his contributions to this Recommendation Guidance.

For questions or assistance, contact Jon P. Yormick, Esq., Yormick Law LLC,
E: jon@yormicklaw.com | M: +1.216.269.5138.