Office of National Drug Control Policy
National HIDTA Program Office

HIDTA Program Guidance for Implementation of the Federal Grantee Provisions In the National Defense Authorization Act

May 8, 2020

TABLE OF CONTENTS

1.0 Background

Effective January 3, 2020, Section § 889(b)(2) of the John McCain National Defense Authorization Act (NDAA) for FY 2019 prohibits executive agencies that administer loan or grant programs from permitting their funds to be used to purchase certain telecommunications and video surveillance equipment and services produced by certain Chinese entities. This applies to Executive Branch agencies like the Office of National Drug Control Policy (ONDCP) and Federal grantees, including the High Intensity Drug Trafficking Areas (HIDTA) Program.

The purpose of this legislation is to reduce the vulnerabilities of Federal agencies and their grantees to foreign interference in technology, data, and operations that rely on telecommunications or video surveillance. The covered telecommunications equipment or services[1] include equipment manufactured or services provided by the following Chinese entities, and their subsidiaries or affiliates:

- Huawei Technologies Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company

Types of prohibited items include (but are not limited to) equipment that can be used to route or redirect user data traffic or permit visibility into any user data or packets that the equipment transmits or otherwise handles. Prohibitions also include telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

2.0 Impact on the HIDTA Program

The provisions of Section § 889(b)(2) of the NDAA prohibit the use of HIDTA funds to purchase items and services that are commonly acquired by law enforcement agencies at all levels of government. Specifically, the prohibition covers equipment or services capable

[1] For additional information on these prohibitions, refer to Section § 889(b)(2) of the John McCain National Defense Authorization Act (NDAA) for FY 2019: https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf

of routing or redirecting user data, or that permits visibility of such data to prohibited foreign vendors. This prohibition could have significant ramifications on task force operations, intelligence sharing, and other HIDTA-funded activities.

Currently, other than the five entities listed above and their subsidiaries and affiliates, there are no applicable Federal prohibitions on specific vendors, their subsidiaries, or affiliates. Beyond the specific vendors listed in the NDAA, other vendors not listed in the statute may present potential security threats to law enforcement operations. Both the ONDCP National HIDTA Program Office (NHPO) and individual HIDTAs must be diligent in vetting current and future vendors for the same security concerns regarding foreign interference, exploitation or theft of sensitive information.

3.0 Actions Taken by NHPO

As of April 2020, the NHPO has taken initial steps to eliminate current telecommunications and equipment providers that pose a national security threat, as well as prohibit the future purchase of such services. In addition to conducting initial reviews of HIDTA inventory for banned telecommunications and other information technology systems and services, NHPO has:

1. Updated the HIDTA Program Policy and Budget Guidance (PPBG) to reflect the prohibited items (refer to section 7.20 Prohibited Use of HIDTA Funds, pg. 46);

2. Coordinated with the HIDTA Directors Committee (HDC), Intelligence Committee, the HDC IT Committee, and the Criminal Intelligence/Information Technology (CI/IT) Crossroads Committee;

3. Engaged directly with the Office of the Director of National Intelligence (ODNI) and the National Counterintelligence Security Center (NCSC) on NDAA implementation and threat mitigation efforts;

4. Completed a preliminary review of HIDTA budget documentation for references to prohibited items and services; and

5. Included the prohibited items and services in fiscal year (FY) 2021 official grant notifications that will be issued to all HIDTA grant recipients.

Based on the information gleaned from these steps, NHPO perceives the risk of foreign interference to be low for the HIDTA Program at this time. However, the level of perceived

risk may vary based on new information, additional statutory prohibitions or Federal regulations, or the emergence of new foreign interference techniques and other vulnerabilities.

In order to mitigate the risk to the HIDTA Program, the NHPO will continue to engage directly with legal counsel and Federal partners to anticipate potential impacts of the NDAA, and identify future areas of concern in systems and services relevant to the law enforcement community. Additionally, the NHPO will monitor legislation and other regulatory actions to determine impact on the HIDTA Program, and communicate requirements to the HIDTA community in a timely fashion.

4.0 Immediate Actions Required of HIDTAs

The prohibition covers equipment or services capable of routing or redirecting user data, or that permits visibility of transmitted user data or packets, from the prohibited foreign vendors. Within 120 days of the release of this memorandum, HIDTAs are required to conduct a review of their current equipment inventories and service contracts to determine whether HIDTA grant funds have been used to purchase equipment or services from prohibited vendors, their affiliates, or subsidiaries. Detailed instructions are provided in Appendix A.

If a HIDTA has used HIDTA grant funds to purchase covered equipment, section § 889(b)(2) of the NDAA requires the NHPO to prioritize assistance to those HIDTAs to replace covered equipment or services. Although the NDAA does not provide a specific timeline for replacing previously purchased covered equipment, the NHPO will prioritize available funds and technical support to assist grantees in transitioning away from using covered equipment, including establishing a plan with regional HIDTAs to phase-out the use of covered equipment over a reasonable period of time.

5.0 Implementing Due-Diligence Practices for NDAA Compliance

NHPO recognizes that it is impossible to identify every potential foreign threat. However, responsible actions by HIDTAs in partnership with participating agencies and fiduciaries can lower the overall risk to an individual HITDA and the HIDTA Program.

This prohibition is likely going to remain as a permanent requirement for all Federal grantees. As information or other resources become available, NHPO will provide updates

and issue guidelines or requirements to the HIDTA Directors via email, and post all relevant documentation to the HIDTA Resource Management System (HRMS).

Going forward, due diligence will be expected of every HIDTA to protect against foreign interference in law enforcement operations. Beyond the requirements and additional recommendations outlined in this memorandum, it is imperative that HIDTAs establish the practice of conducting research into vendors, equipment, and services for potential vulnerabilities, and work with fiduciaries and partner agencies to ensure acquisition protocols and procedures incorporate considerations related to NDAA compliance.

To assist HIDTAs in assuming a posture that reduces vulnerabilities associated with foreign interference, this memorandum contains general guidelines that HIDTAs may adopt. For information on protocols that may assist in vetting potential vendors, refer to Appendix B. Additional information resources, including approved vendor lists from U.S. Department of Defense (DoD) can be found in Appendix C. Finally, Appendix D offers guidance and a checklist for HIDTA management teams and initiative commanders to complete before purchasing covered items and services with HIDTA funds, and Appendix E contains general language that can be used to notify fiduciaries of the NDAA provisions applicable to the HIDTA funds they administer.

APPENDICES

Appendix A: HIDTA Inventory Review Procedures (Required Action)

In order to fully comply with the provisions of Section § 889(b)(2) of the NDAA, each HIDTA must complete the following actions within 120 days of the issuance of this memorandum.

Step 1: Inventory Review

Review the equipment inventory for the specific vendors and associated items listed in section § 889(b)(2) of the NDAA, to include their affiliates and subsidiaries (if known):

- Huawei Technologies Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company

Step 2: Contract Review

Review current service contracts for the specific vendors and associated services listed in section § 889(b)(2) of the NDAA, to include their affiliates and subsidiaries (if known).

Step 3: Notification to ONDCP

If the review does not identify prohibited equipment, the HIDTA must notify ONDCP via email sent to ONDCP_HIDTA@ondcp.eop.gov that states the following:

> "[Insert] HIDTA has completed the required inventory review, and hereby affirms that no prohibited items or services under section § 889(b)(2) of the NDAA were found to be in the possession or employ of the [insert] HIDTA."

If prohibited equipment or service contracts are found, the HIDTA must notify NHPO within 5 business days of identifying the items or services. The notification should be sent to ONDCP_HIDTA@ondcp.eop.gov and include the following:

- Subject line – "NDAA Prohibited Item Notification"
- Email body –
  - Item make/model
  - Year purchased (if known)

  - Applicable grant number
  - Cost at time of purchase, along with estimated depreciation

- Any service contracts with prohibited vendors should also be identified by providing the following –
  - Vendor
  - Brief description of the service
  - Length/timeframe of the executed contract
  - Associated cost(s)

If the notification includes multiple items, the HIDTA may submit all items in an Excel spreadsheet.

Step 4: Notify the Executive Board

Notify the Executive Board that these actions have been completed, along with any follow-on directives from ONDCP.

Step 5: Notify All Fiduciaries

Ensure fiduciaries are notified (see Appendix E) and that initiative commanders are provided with applicable guidance (see Appendix D), as appropriate.

Step 6: Revise and Update Materials

Revise the new Executive Board member and initiative commander orientation materials to reflect the requirements outlined in this memo, along with the due diligence recommendations and any additional guidance issued by the HIDTA or the fiduciaries pertaining to NDAA compliance.

Appendix B: Due Diligence Recommendations

In addition to any forthcoming recommendations or guidelines, HIDTAs are expected to perform due diligence when procuring equipment or services to minimize the risk of foreign interference. At a minimum, the NHPO recommends the following practices be implemented by each HIDTA.

Verify Vendor Information

When making procurement decisions, leverage open source materials and search engines (e.g., Google, Bing, etc.) to identify vendors approved by Federal Government entities, as well as potential causes for concern in open source information:

- Use additional resources below from the U.S. General Services Administration (GSA), Department of Defense Information Network (DoDIN), Bureau of Industry and Security at the U.S. Department of Commerce (BIS), and the National Counterintelligence Security Center (NCSC) (see Appendix C for links to this information);
- Conduct searches for news articles, Federal Government notifications and information on threats emanating from foreign countries, or legal/regulatory actions taken against firms that fail to protect information from foreign interference for specific telecommunications or video surveillance equipment purchases; and
- Search records and see if vendor is registered in the Office of Personnel Management's System for Award Management (SAM) at www.sam.gov

Enhance Inventory Tracking

Update the annual inventory review process to include the list of prohibited items, as well as additional information on equipment to expedite future inventory reviews (e.g., in the event that additional vendors are added to prohibited lists):

- Include more detailed descriptions of all telecommunications and video surveillance equipment and services, including model and manufacturer
- Add the following to inventory databases for all telecommunications and video surveillance equipment:

- Vendor Name
- Vendor Address
- Vendor and/or Product Website

Inform and Continuously Update Initiative Commanders

Update initiative commanders as part of their annual refresher training on prohibited vendors, or services and equipment that may require additional vetting and research. Include the *Initiative Commander NDAA Pre-Purchase Checklist* (Appendix D) with all new initiative commander training(s) offered by the HIDTA.

Appendix C: Additional Information and Resources

HIDTA management teams should become familiar with the following resources, and refer to the publicly available vendor lists. Note that these are the only vendor lists issued by the Federal Government at this time. As more Federal Government resources become available, NHPO will issue them to the HIDTAs, and post documents on HRMS.

General Information about the NDAA

- National Defense Authorization Act (NDAA) FY 2019 - https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf
- NDAA Legislative History - https://www.congress.gov/115/crpt/hrpt676/CRPT-115hrpt676.pdf
- United States Department of Justice Press Release of Huawei Technologies Co., Ltd.'s indictment - https://www.justice.gov/usao-edny/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering

Federal Government Vendor and Entity Lists

- U.S. General Services Administration (GSA) Approved Manufacturer List -

  https://www.gsaadvantage.gov/advantage/s/mfr.do?q=0:2gs-35f-0119y&db=0&searchType=1&listFor=All

  - GSA serves as the acquisition and procurement arm of the Federal government, offering equipment, supplies, telecommunications, and integrated information technology solutions to Federal agencies so that the agencies can focus on serving the public. This is a link to vendors they have already approved.

- Department of Defense Information Network (DoDIN) Approved Products List (APL) – https://aplits.disa.mil/processAPList.action

  - This is updated periodically and a PDF version is available for download
  - The Department of Defense Information Network (DoDIN) Approved Products List (APL) is the single consolidated list of products that have completed Cybersecurity (CS) and Interoperability (IO) certification

- Bureau of Industry and Security (BIS) at the U.S. Department of Commerce Entity List – https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file

    - BIS first published the Entity List in February 1997 as part of its efforts to inform the public of entities who have engaged in activities that could result in an increased risk of the diversion of exported, re-exported and transferred (in-country) items to weapons of mass destruction (WMD) programs. Since its initial publication, grounds for inclusion on the Entity List have expanded to activities sanctioned by the State Department and activities contrary to U.S. national security and/or foreign policy interests.

Information about Foreign Interference, Supply Chain Security, and Cybersecurity

- National Counterintelligence Security Center (NCSC) public website – https://www.dni.gov/index.php/ncsc-home

Appendix D: NDAA Pre-Purchase Checklist

To ensure the exercise of due diligence when procuring items or services that may be covered by Section § 889(b)(2) of the NDAA, HIDTA management teams and initiative commanders should first determine whether the equipment or service meets one or both of the following criteria:

1. Does the equipment or service include the capture or storage of digital information or imagery (e.g. surveillance footage, or drones and drone images, etc.)?

2. Does the equipment or service transmit information or communications electronically (e.g. two-way radios, data sharing services, etc.)?

If the answer to one or both questions is "yes," then the equipment or service is likely covered by the NDAA and subject to additional scrutiny. At a minimum, HIDTAs must ensure that the equipment or service is not manufactured, maintained, or otherwise associated with a covered foreign entity (reference the list of prohibited vendors in Appendix A). In addition, HIDTA management teams and initiative commanders should strive to answer the following questions prior to procuring any covered equipment or service with HIDTA funds:

1. Is the vendor based within the United States?

2. Does the vendor source components for the equipment or services from within the United States?

3. Is data stored and maintained within the United States?

4. Are warranty or service agreements honored or fulfilled within the United States?

5. Relying upon the best available information, is the vendor, including its affiliates or subsidiaries not listed as prohibited in HIDTA Program Policy and Budget Guidance (PPBG)?

An answer of "yes" to each of the above questions represents the lowest level of perceived risk to an individual HIDTA and the HIDTA Program. A "no" answer to any of the above questions may warrant additional review by the initiative commander and/or the HIDTA Director (or their designee) to determine the level of risk posed by procurement of the equipment or service.

Whenever procuring equipment or services from foreign vendors (e.g., the vendor website references China or Chinese entities, or any other foreign entities), included non-prohibited vendors, the HIDTA should determine the following before procuring the equipment or service:

- Is the equipment or service essential?
- Is a viable alternative manufactured or otherwise provided in the United States?
- Is any open source information readily available (e.g., internet search, news articles) that identifies potential risks posed by the equipment or service?

Although the only prohibited vendors are those outlined in the PPBG and this document, HIDTA management teams and initiative commanders should take every reasonable precaution to ensure that equipment and services purchased from foreign vendors do not unnecessarily increase vulnerability. By conducting due diligence HIDTAs are better positioned to identify potential threats and vulnerabilities, and manage risks.

HIDTAs may adapt portions of this guidance into their own materials and formatting, as appropriate. It is recommended that HIDTAs incorporate this guidance and the checklist to initiative commanders during their orientation to the HIDTA, and on an annual basis thereafter.

Appendix E: Fiduciary Notice of NDAA Prohibitions Applicable to HIDTA Grantees

Effective January 3, 2020, Section § 889(b)(2) of the John McCain National Defense Authorization Act (NDAA) for fiscal year (FY) 2019 prohibits executive agencies that administer loan or grant programs from permitting their funds to be used to purchase certain telecommunications and video surveillance equipment and services produced by certain Chinese entities. This prohibition extends to Federal grant programs, including the High Intensity Drug Trafficking Areas (HIDTA) Program.

The purpose of this legislation is to reduce the vulnerabilities of Federal agencies and their grantees to foreign interference in technology, data, and operations that rely on telecommunications or video surveillance. As a fiduciary for the (insert) HIDTA, you are required to observe the provisions outlined in the NDAA for all expenditures of HIDTA grant funds. While no immediate action is required, compliance with the NDAA necessitates that HIDTA fiduciaries work with the (insert) HIDTA leadership to determine the overall impact of these prohibitions on acquisition and procurement activities involving HIDTA funds.

At a minimum, covered telecommunications equipment or services[2] include equipment manufactured or services provided by the following Chinese entities, and their subsidiaries or affiliates:

- Huawei Technologies Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company

Types of prohibited items include (but are not limited to) equipment that can be used to route or redirect user data traffic or permit visibility into any user data or packets that the equipment transmits or otherwise handles. Prohibitions also include telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the

[2] For additional information on these prohibitions, refer to Section § 889(b)(2) of the John McCain National Defense Authorization Act (NDAA) for FY 2019: https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf

Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

At this time, the Office of National Drug Control Policy (ONDCP) assesses the overall risks associated with foreign interference and compliance with the NDAA to be low for the HIDTA Program. However, all HIDTAs have been instructed to take initial steps to ensure compliance with the provisions of the law, and to implement due diligence practices that minimize vulnerabilities to foreign interference through technology acquisitions in support of law enforcement operations and data sharing.

As of this notification, the Federal Government has not provided a detailed list of prohibited vendors (other than those named in the legislation, and listed above), affiliates, or subsidiaries. However, the (insert) HIDTA will continually monitor directives from ONDCP and other Federal entities for updates to the prohibitions outlined above and share them with you as quickly as possible.

Please direct any further questions to (insert).