

PROPOSED CHARGING LETTER

Mr. Peter C. Gundersen, Jr.
Corporate Vice President, Global Trade
RTX Corporation
1000 Wilson Blvd.
Arlington, VA 22209

Re: Violations of the Arms Export Control Act and the International
Traffic in Arms Regulations by RTX Corporation

Dear Mr. Gundersen:

The Department of State (Department) charges RTX Corporation, including its operating divisions, subsidiaries, and business units (collectively “RTX” or “Respondent”), with violations of the Arms Export Control Act (AECA) (22 U.S.C. 2751 *et seq.*) and the International Traffic in Arms Regulations (ITAR) (22 C.F.R. parts 120-130) in connection with unauthorized exports, reexports, and retransfers of defense articles to multiple countries, including proscribed destinations listed in 22 C.F.R. 126.1; and violations of license terms, conditions, and provisos of Directorate of Defense Trade Controls (DDTC) authorizations. A total of 750 violations are charged at this time.

The essential facts constituting the charged violations are described herein. The Department reserves the right to amend this proposed charging letter, including through a revision to incorporate additional charges stemming from the same misconduct of Respondent. Please be advised that this proposed charging letter, pursuant to 22 C.F.R. 128.3, provides notice of the Department’s intent to impose civil penalties in accordance with 22 C.F.R. 127.10.

When determining the charges and penalties to pursue in this matter, the Department considered mitigating factors. Most notably: (a) Respondent voluntarily disclosed the violations, the majority of which resulted from historical systemic failures in an acquired company’s ITAR compliance program that predated Respondent’s 2018 acquisition of the company; (b) Respondent cooperated with the Department’s requests for information; (c) Respondent entered into multiple agreements with the Department tolling the statutory period that applies to enforcement of the AECA and the ITAR; (d) Respondent continues to invest significant resources in its export compliance program in order to remediate

and prevent the recurrence of the violations described herein; and (e) Respondent has taken substantial steps to enhance the acquired company's ITAR compliance processes and integrate it into Respondent's corporate export compliance program.

The Department notes that had the Department not taken into consideration these mitigating factors, it would have charged Respondent with additional violations or proposed a higher penalty. In particular, the Department has elected to reduce the number of violations associated with the acquired company in recognition of Respondent's role, and transparent and cooperative approach with DDTC, in identifying and reporting those violations.

When determining the violations to pursue in this matter, the Department also considered aggravating factors, including: (a) harm to U.S. national security; (b) unauthorized exports of classified defense articles; (c) unauthorized exports to proscribed destinations listed in 22 C.F.R. 126.1, including Iran, Lebanon, Russia, and the People's Republic of China (PRC);¹ (d) unauthorized exports of defense articles, including technical data, designated as Significant Military Equipment (SME);² and (e) the recurrence of violations after Respondent implemented corrective actions to address the root causes of those violations.

This proposed charging letter describes violations for the time period from August 5, 2017, to September 29, 2023.

JURISDICTION

Respondent is a corporation organized under the laws of Delaware and a U.S. person within the meaning of 22 C.F.R. 120.62. Respondent is subject to the jurisdiction of the United States.

During the period covered by the violations set forth herein, Respondent was engaged in the manufacture, brokering, and export of defense articles and was

¹ Certain violations occurred prior to Russia's addition to 22 C.F.R. 126.1 on March 18, 2021. However, at the time of some of these violations, Russia was subject to restrictive measures on defense exports per the Department of State press release of April 28, 2014, "United States Expands Export Restrictions on Russia" (available at: <https://2009-2017.state.gov/r/pa/prs/ps/2014/04/225241.htm>).

² As defined in 22 C.F.R. 120.36, SME means articles for which special export controls are warranted because of their capacity for substantial military utility or capability. Pursuant to 22 C.F.R. 120.10(c), technical data directly related to the manufacture or production of a defense article designated as SME is also designated as SME. Additionally, pursuant to 22 C.F.R. 120.36(b)(2), all classified defense articles are also designated as SME.

registered with DDTC as a manufacturer, broker, and exporter, in accordance with section 38 of the AECA and 22 C.F.R. 122.1 and 129.3.

The described violations relate to defense articles controlled under Categories II(k), IV(a), IV(c), IV(h), IV(i), VI(f), VI(g), VII(h), VIII(g), VIII(h), VIII(i), IX(b), X(a), X(e), XI(a), XI(c), XI(d), XII(c), XII(d), XII(e), XII(f), XIII(b), XIII(l), XIX(f), and XIX(g) of the U.S. Munitions List (USML), 22 C.F.R. 121.1, at the time the violations occurred.

BACKGROUND

RTX is a multinational aerospace and defense company headquartered in Arlington, Virginia. On April 3, 2020, United Technologies Corporation (UTC) and Raytheon Company completed a merger transaction whereby Raytheon Company survived as a corporate entity and became a wholly-owned subsidiary of UTC, and UTC changed its corporate name to Raytheon Technologies Corporation. On July 17, 2023, RTX completed a rebranding and name change whereby Raytheon Technologies Corporation became RTX Corporation. RTX now consists of three primary operating divisions:

- Collins Aerospace (Collins) is headquartered in Charlotte, North Carolina and designs, manufactures, and services aerospace systems. It also provides integrated-system solutions and services for commercial, regional, corporate, and military aircraft. UTC acquired Rockwell Collins, Inc. (Rockwell Collins) in November 2018 and combined it with UTC Aerospace Systems to form Collins.
- Pratt & Whitney (P&W) is headquartered in East Hartford, Connecticut, and designs, manufactures, and services commercial and military aircraft engines.
- Raytheon (RAY) is headquartered in Arlington, Virginia and develops and produces advanced sensors, cyber and software solutions, air and missile defense systems, precision weapons, and radars and command and control systems. On July 1, 2023, RTX combined its operating businesses, Raytheon Intelligence & Space and Raytheon Missiles and Defense, to become RAY.

The Department notes that the majority of violations described herein resulted from historical systemic failures in Rockwell Collins' export control compliance program. While all of Respondent's affiliates committed a substantial number of violations, pervasive ITAR compliance weaknesses at Rockwell Collins resulted in many of the most egregious violations such as unauthorized exports of technical data to the PRC to facilitate procurement of defense articles from Chinese entities.

VIOLATIONS

The ITAR violations described herein are derived from 113 voluntary disclosures that Respondent submitted to DDTC in accordance with 22 C.F.R. 127.12 for activities between August 2017 and September 2023. Due in part to the large number of violations over an extended period of time, the Department provides a summary of the violations, which fall into four broad categories: 1) unauthorized exports of defense articles resulting from the failure to establish proper jurisdiction and classification; 2) unauthorized exports of defense articles, including classified defense articles; 3) unauthorized exports of defense articles by employees via hand-carry to proscribed destinations listed in 22 C.F.R. 126.1; and 4) violations of terms, conditions, and provisos of DDTC authorizations. The majority of violations resulting from jurisdiction and classification errors, in particular, reflect a clear pattern of historical systemic compliance failures in multiple of Respondent's operating divisions. In some instances, these operating divisions failed to fully remediate these failures.

The Department previously identified similar categories of violations in Proposed Charging Letters (PCL) to both of Respondent's predecessor companies. In its 2013 PCL to Raytheon Company, the Department separated the company's violations into two broad categories: "1) failure to properly manage Department-authorized agreements; and 2) failure to properly manage temporary export and import authorizations." The Department also observed "a corporate-wide weakness in . . . investigating and correcting errors that require[d] immediate, comprehensive, effective remedial action across [Raytheon Company's] many operating units and subsidiaries." The Department also referenced specific instances wherein Raytheon Company "described a number of corrective actions for [one] business unit, but did not prescribe corrective actions for other business units that may have similar pervasive issues."

Similarly, the Department's 2012 PCL to UTC identified three broad categories of violations: "1) unauthorized exports and reexports resulting from the

failure to properly establish jurisdiction over defense articles and technical data; 2) unauthorized exports resulting from the failure to exercise internal controls over technical data; and 3) failure to properly manage Department-authorized agreements.” The Department noted that UTC’s subsidiaries “repeatedly discovered and disclosed violations to the Department, in some cases finding that reported remedial measures failed to prevent or detect additional similar violations.” Similar violations occurred following the conclusion of Raytheon Company’s and UTC’s most recent Consent Agreements in 2018 and 2016, respectively.

The Department notes that, since the closing of the prior Consent Agreements, Respondent has dedicated significant resources to sustain and improve its export compliance program and has worked to integrate companies it has acquired into that program. This includes investing significant resources in personnel and systems for the monitoring and auditing of ITAR compliance, and for the identification, reporting, investigation, and disclosure of potential ITAR violations. These investments were critical in identifying and remedying the violations described herein. Respondent has, nevertheless, committed numerous ITAR violations, as described below.

I. Unauthorized Exports, Reexports, Retransfers, and Temporary Imports Resulting from the Failure to Establish Proper Jurisdiction and Classification

Since 2020, Respondent has submitted 27 voluntary disclosures to the Department demonstrating systemic failures to establish proper jurisdiction and classification of defense articles within certain operating divisions. As a result, Respondent without authorization exported and caused to be reexported a substantial number of defense articles to 32 different countries, including to the PRC, a proscribed destination listed in 22 C.F.R. 126.1. Respondent or its foreign affiliates also without authorization retransferred misclassified defense articles within foreign countries and temporarily imported without authorization defense articles from foreign countries to the United States. In at least two cases, such unauthorized exports resulted in the manufacture of thousands of defense articles (comprising approximately 45 distinct part numbers) in the PRC, importation of those defense articles into the United States, and the eventual integration of those defense articles into multiple U.S. and partner military platforms. In 16 cases, Respondent or its foreign affiliates exported or reexported without authorization defense articles related to military aircraft and missile system programs, including SME. In multiple cases, Respondent acknowledged that it failed to keep complete records related to the disclosed violations as required by 22 C.F.R. 122.5. This

occurred because Respondent had incorrectly established that the relevant defense articles were controlled under the Export Administration Regulations (EAR), thus potentially resulting in additional undisclosed ITAR violations. The majority of these voluntary disclosures and violations arose out of jurisdiction and classification errors made by Rockwell Collins prior to its acquisition by UTC.

Unauthorized Exports to the PRC Resulting from Misclassification

Respondent disclosed that it exported without authorization technical data to the PRC on numerous occasions between 2014 and 2023 predominantly because of a historical misinterpretation by Rockwell Collins of the ITAR's "specially designed" definition and release criteria in 22 C.F.R. 120.41. Respondent corrected this misinterpretation through integration of Rockwell Collins into its corporate ITAR compliance program, however Respondent continued to discover and, in some cases, commit violations stemming from these historical errors.

In two disclosures that Respondent initially submitted to the Department in 2021 and 2022, it disclosed unauthorized exports that occurred at Respondent's facility in Cedar Rapids, Iowa, in the form of unauthorized releases of USML Category VIII(i) technical data related to the Boeing E-3 Sentry Airborne Early Warning and Control Aircraft and the Embraer KC-390 Millennium Medium Weight Transport Plane to Chinese foreign-person employees (FPE). Respondent identified the root cause of these violations as Rockwell Collins' "historical misinterpretation" and "general misunderstanding" of the ITAR's specially designed definition and release criteria in 22 C.F.R. 120.41. To address this root cause, Respondent implemented corrective actions to improve compliance training and integrate the relevant acquired business into Respondent's broader corporate ITAR compliance program.

In a subsequent disclosure submitted to the Department in 2023, Respondent disclosed that in January 2023 it exported without authorization USML Category VIII(i) technical data, misclassified in March 2018, related to an aluminum display housing component of the F-22 Raptor Fighter Aircraft to two Chinese FPEs at Collins' facility in Shanghai, PRC. Respondent also contemporaneously and separately exported without authorization the same technical data to four entities in the PRC as part of a Request for Quotation (RFQ). Respondent's employees assessed that the F-22 component and related technical data were EAR99 but later determined that the technical data "instead should have been classified under the ITAR under USML Category VIII(i)." Respondent determined that the root cause of these violations was the same historical misinterpretation of the specially

designed definition set forth in 22 C.F.R. 120.41. Respondent indicated that it had “implemented a range of corrective actions over the past two-plus years to fully integrate heritage [Rockwell Collins] businesses into [Respondent’s] jurisdiction and classification program,” and stated that the corrective actions were intended to “prevent similar violations from occurring in the future.”

In a separate 2023 disclosure, Respondent described a jurisdiction and classification review that it undertook following the discovery of the systemic violations described in the previous paragraphs. The review revealed that between March 2015 and May 2023 Respondent exported without authorization USML Category XI(d) technical data to Chinese entities, again as part of RFQs. Respondent disclosed that these violations “arose from incorrect classifications” that were “largely the result of [Rockwell Collins’] misinterpretation of the ITAR Section 120.41(b)(4) release.” In explaining these additional failures to properly establish the jurisdiction and classification of defense articles, Respondent described a 2015 memorandum contemplating a potential commercial, i.e., non-ITAR-controlled, usage of certain circuit card assemblies that did not ultimately come to fruition. Respondent disclosed that “[i]n reliance on this memo, [Rockwell Collins] released certain circuit card assemblies . . . from the ITAR in accordance with Section 120.41(b)(4), based on an assumption that the circuit card assemblies would be used on a commercial radio in the future.”

Unauthorized Procurement from the PRC Resulting from Misclassification

Respondent disclosed that between 2015 and 2023, Rockwell Collins and, for a period following the acquisition, Collins, exported without authorization technical data controlled under USML Category XI(d) to entities in the PRC in order to procure approximately 45 distinct USML Category XI(c)(2) printed wiring boards (PWBs) that had been historically misclassified by Rockwell Collins, again due to the misapplication of the specially designed release criteria in 22 C.F.R. 120.41. Following these exports, Rockwell Collins (and subsequently Collins) issued purchase orders to procure thousands of these PWBs from those PRC entities. Subsequently, Rockwell Collins (and Collins) delivered these PWBs to other prime contractors and directly to U.S. Department of Defense (DoD) customers for ultimate end use in U.S. and foreign military platforms, including but not limited to the:

- VC-25 Presidential Transport Aircraft (Air Force One);
- A-10 Thunderbolt II Close Air Support Attack Aircraft;

- B-1B Lancer Supersonic Strategic Heavy Bomber;
- B-52 Stratofortress Strategic Bomber;
- C-17 Globemaster III Strategic Airlifter;
- C-130J Super Hercules Military Transport Aircraft;
- CH-53 Super and King Stallion Cargo Helicopter;
- F-15 Eagle Fighter Aircraft;
- F-16 Fighting Falcon Fighter Aircraft;
- F/A-18 Hornet Fighter Aircraft;
- KC-46 Pegasus Tanker Aircraft;
- KC-130 Tanker Aircraft;
- KC-135 Stratotanker Tanker Aircraft;
- MQ-4 Triton Surveillance Unmanned Aerial Vehicle (UAV);
- MQ-8 Fire Scout UAV Helicopter;
- MQ-9 Reaper Combat UAV;
- MQ-25 Stingray Refueling UAV;
- P-8 Poseidon Maritime Patrol Aircraft; and the
- U-2 Reconnaissance Aircraft

The Department notes that Respondent did not inform its customers, including DoD customers, of the components' origin until months or in some instances years following the first deliveries.

In at least one disclosure, Respondent reported that, following issuance of purchase orders and production of the PWBs by its Chinese suppliers, it caused the retransfer without authorization of technical data in the form of first-article inspection reports to its Chinese FPEs in Shanghai. Respondent disclosed that its processes "did not prevent the issuance of these purchase orders because the commodity being sourced from outside the United States (and related technical data) had been incorrectly identified as being subject to the EAR and eligible for export as 'no license required.'" Respondent identified the root cause of these violations as the same historical incorrect application and misinterpretation of specially designed release criteria set forth in 22 C.F.R. 120.41.

Harm to National Security

In a 2023 disclosure, Respondent disclosed that, predominantly as a result of misclassifications UTC Aerospace Systems made between 2013 and 2017, it exported without authorization USML Category VIII(i) technical data to entities in

multiple foreign countries, including the PRC, as part of RFQs between 2019 and 2021. Respondent also disclosed that, at the time of the exports, it had incorrectly classified the technical data, which related to the environmental control system of the F/A-18 E/F Super Hornet, under the EAR. Respondent also disclosed that the misclassifications occurred because the work instruction given to classifiers before 2017 “provided no guidance on how to interpret and apply the ITAR Section 120.41(b)(3) release.”

The U.S. government reviewed copies of the technical data that Respondent exported without authorization and concluded that certain exports to the PRC harmed U.S. national security. Specifically, the U.S. government concluded that certain unauthorized exports provided insight into design methodology, design analysis, and manufacturing know-how associated with environmental control system components for F/A-18 E/F Super Hornet and the EA-18G Growler military aircraft, thereby harming U.S. military programs and providing the recipients with a capability they had not previously held.

Unauthorized Exports Related to Sensitive Military Platforms Resulting from Misclassification

Respondent disclosed that between August 2017 and August 2022, Raytheon Company, and subsequently RAY, exported without authorization USML Category IV(c), IV(h), VI(f), XI(c), XI(d), and XII(e) defense articles to Australia, Belgium, Canada, France, Germany, Greece, Israel, Japan, Mexico, the Netherlands, the Republic of Korea, Saudi Arabia, Singapore, Sweden, Türkiye, the United Arab Emirates (UAE), and the United Kingdom. The unauthorized exports comprised parts, components, and technical data related to sensitive U.S. and foreign government military platforms, including but not limited to the:

- Tomahawk Cruise Missile;
- RIM-162 Evolved SeaSparrow Missile (ESSM);
- RIM-116 Rolling Airframe Missile;
- Standard Missile-2; and the
- PAVEWAY Laser-Guided Bomb

In its disclosures, Respondent identified multiple root causes of these violations, including RAY’s: 1) misapplication of the “specially designed” release set forth in 22 C.F.R. 120.41; 2) failure to apply the “see-through rule” to defense

articles;³ 3) failure to provide specific guidance regarding specially designed hardware to engineers performing jurisdiction and classification assessments prior to May 2018; and 4) failure to properly conduct an Order of Review on hardware that may contain lower-level assemblies subject to the ITAR.

Unauthorized Reexports, Retransfers, and Temporary Imports Resulting from Misclassification

In seven disclosures, Respondent reported that its failure to establish proper jurisdiction and classification of defense articles resulted in violations committed by its foreign affiliates in France and Germany. Specifically, Respondent's foreign affiliates reexported without authorization defense articles, including SME, to multiple foreign countries and retransferred without authorization defense articles to other entities within France and Germany. Further, Respondent temporarily imported without authorization defense articles into the United States, identifying those defense articles as EAR-controlled on various import documents.

In summary, despite the fact that Respondent implemented corrective actions in each of the abovementioned disclosures to address the root cause of its jurisdiction and classification issues, it continued to discover – and in some cases continued to commit – violations resulting from historical incorrect jurisdiction and classification determinations, the majority of which were made by Rockwell Collins prior to its acquisition by UTC in 2018. In one particular case, Respondent disclosed that its investigation found that the Global Trade (GT) department, including leadership of both Respondent's pre-merger affiliate, Raytheon Missile Systems (RMS), and Raytheon Company Corporate, had knowledge of RMS's ITAR §120.41(b)(3) failures and did not take appropriate measures to mitigate potential violations resulting from RMS's reliance on erroneous classifications.

II. Unauthorized Exports, Reexports, and Retransfers of Defense Articles, including Classified Defense Articles

Since 2019, Respondent has submitted dozens of voluntary disclosures to the Department describing additional unauthorized exports of defense articles, including classified defense articles.

³ 22 C.F.R. 120.11(c), commonly referred to as the “see-through rule,” states that “[d]efense articles described on the USML are controlled and remain subject to this subchapter following incorporation or integration into any item not described on the USML, unless specifically provided otherwise in this subchapter.”

Unauthorized Exports of Classified Defense Articles

In four disclosures, Respondent disclosed that it exported without authorization classified defense articles controlled under USML Categories IV(h), IV(i), and XI(c) to Australia, Germany, Norway, and the UAE related to the following programs:

- National Advanced Surface-to-Air Missile System;
- RIM-162 Evolved SeaSparrow Missile;
- Tomahawk Cruise Missile; and
- AIM-120 Advanced Medium-Range Air-to-Air Missile Extended Range (AMRAAM-ER)

Harm to National Security

Respondent disclosed that in October 2020, it exported without authorization USML Category IV(i) classified technical data to Norway. Respondent disclosed that the unauthorized export occurred because its employees “were confused about which document was to be sent” to the intended recipient despite specific instructions and “the obvious [classification] markings” on the document that they exported without authorization. The U.S. government reviewed copies of the files referenced in this disclosure and determined that the unauthorized export of classified technical data harmed U.S. national security.

Additional Unauthorized Exports of Classified Defense Articles

In a 2021 disclosure, Respondent described its unauthorized temporary exports of classified components related to the ESSM to Australia and Germany. In July 2020, Respondent prepared to temporarily export eight unclassified USML Category IV(h) transition sections for the ESSM Block 1 Guided Missile Assembly to Germany for repair under a DSP-73 authorization. Two of the eight transition sections included “erroneously installed” USML Category IV(h) S-Band Transceiver Modules (SBT), which are classified, designated SME, and were not authorized for temporary export under the DSP-73. When preparing the transition sections for export, quality inspection personnel at Respondent’s Tucson, Arizona facility noticed classified markings on two of the transition sections and, on two occasions, requested clarification from ESSM program personnel regarding the classification status of those sections. The ESSM hardware lead “replied that she believed the SBTs had been removed from the Transition Sections” and, as a

result, were “unclassified.” The quality inspector “trusted the response that the SBTs were unclassified and finalized the inspection.” Subsequently, Respondent exported the SBTs to Germany without authorization. Respondent disclosed that “[u]p until the incident timeframe, there was not a documented process to require the removal of an SBT from a Transition Section prior . . . to export to [Germany]” and that “because the part numbers for Transition Sections with and without SBTs installed were identical, [RAY’s] asset tracking system did not otherwise distinguish between the classified and unclassified versions of the Transition Sections.”

In the same disclosure, Respondent disclosed the unauthorized export of one classified USML Category XI(c) “erroneously installed” hard drive to Australia. In September 2019, Respondent prepared to export to Australia an oscilloscope intended for use with the MK698 Guided Missile Test Set in support of the ESSM program. Following pre-export tests using the classified hard drive, Respondent’s policy required the “sanitization” of the oscilloscope, i.e., removal of the hard drive, and the updating of classified markings on the oscilloscope prior to export. Respondent disclosed that, in preparation for the eventual export of the oscilloscope, the ESSM engineer and safe custodian tasked by the ESSM technical lead to prepare the oscilloscope for export “did not sanitize the oscilloscope” and “did not update the classification markings on the exterior of the oscilloscope” because they were “distracted by other priorities.” Another technical lead later “confirmed that the oscilloscope was ready for shipment” but “did not inspect the oscilloscope for the hard drive or otherwise verify [that the] sanitization procedure was followed.” Respondent subsequently exported the classified hard drive without authorization to Australia in October 2019.

In a 2023 disclosure, Respondent described the unauthorized export of classified USML Category IV(i) technical data to Australia. In November 2021, Respondent exported a CD-ROM intended to include software related to the AMRAAM to its Australian affiliate, Raytheon Australia (RA), under a DDTC authorization. In September 2022, a RA employee notified Respondent “that RA had received an incorrect version of AMRAAM software” and that they “observed the file names on the CD referred to AMRAAM-ER,” which was not authorized for export under the relevant DDTC authorization. Respondent disclosed that “although the physical label on the CD stated ‘AMRAAM’ . . . the CD did not contain the correct software.” In a separate disclosure, Respondent described another unauthorized export of classified USML Category IV(i) technical data related to the AMRAAM-ER to the UAE during an in-person briefing.

In each of these four disclosures, Respondent identified the primary root cause of the violations as individual employees' failures to verify whether the defense articles were classified or approved under the relevant DDTC authorizations prior to the unauthorized exports.

Other Unauthorized Exports, Reexports, and Retransfers of Defense Articles

In 54 disclosures submitted to the Department since 2019, Respondent disclosed that it exported, reexported, and retransferred without authorization hundreds of defense articles, some of which qualified as SME, to or within 25 different countries, including the PRC. The defense articles that Respondent exported, reexported, or retransferred without authorization relate to multiple U.S. and foreign military platforms, including but not limited to the:

- Aegis Ballistic Missile Defense System;
- B-2 Spirit Bomber Aircraft;
- F/A-18 E/F Super Hornet Fighter Aircraft;
- F-15 Eagle Fighter Aircraft;
- F-16 Fighting Falcon Fighter Aircraft;
- F-22 Raptor Fighter Aircraft;
- F-35 Lightning II Fighter Aircraft;
- National Advanced Surface-to-Air Missile System;
- PATRIOT Air Defense System;
- Phalanx Close-In Weapons System; and the
- RIM-116 Rolling Airframe Missile.

The Department notes that the unauthorized exports, reexports, and retransfers described in this section involve each of Respondent's U.S. affiliates and thus demonstrate widespread violations throughout Respondent's ITAR compliance program.

III. Unauthorized Exports of Defense Articles by Employees via Hand-Carry to Proscribed Destinations

Since 2019, Respondent has submitted three voluntary disclosures describing unauthorized exports of defense articles to proscribed destinations during employee travel. In each of these cases, Respondent's employees hand-carried mobile devices containing ITAR-controlled technical data to proscribed

destinations listed in 22 C.F.R. 126.1 during personal travel, in contravention of company policy and internal controls.

Unauthorized Exports to Lebanon

In a 2021 disclosure, Respondent described the unauthorized export of defense articles to Lebanon, a proscribed destination listed in 22 C.F.R. 126.1, during two personal trips one employee took in 2020 and 2021. The employee hand-carried his RTX-issued laptop, which contained ITAR-controlled technical data and was “capable of accessing the Raytheon U.S. network using a secure Virtual Private Network,” on both trips. In preparation for the first trip, the employee submitted a request via the Raytheon Global Export Management System (RGEMS) to bring his laptop but did not list Lebanon as an intended destination on that request. Upon return from the trip in November 2020, the employee annotated his RGEMS entry indicating that he had been rerouted to “Luban” during travel. Respondent reported that the employee who reviewed the updated RGEMS entry failed to appreciate that “Luban” was a reference to the romanized Arabic name for Lebanon “and did not elevate the matter for further investigation.” In April 2021, the same employee submitted a second RGEMS request to bring his laptop and RTX-issued smartphone on personal travel, but again did not list Lebanon as an intended destination. The employee again visited Lebanon and, upon return to the United States, annotated his RGEMS entry to report a stop in “Liban,” i.e., the French name for “Lebanon.” Respondent again “failed to identify and escalate the deviation for investigation.”

Harm to National Security

Respondent discovered these violations during a standard monthly compliance review in July 2021 and, following an internal investigation, determined that the employee’s laptop contained USML Category IV(i) technical data related to the Standard Missile-3, Standard Missile-6 (SM-6), and ESSM Block 2. The U.S. government reviewed copies of the files referenced in this disclosure and determined that the unauthorized export of technical data harmed U.S. national security and adversely impacted a DoD Program of Record.

Unauthorized Exports to Russia

In a 2022 disclosure, Respondent described the unauthorized exports of defense articles to Russia, a proscribed destination listed in 22 C.F.R. 126.1, during one employee’s personal trip in May and June of 2021. The employee hand-

carried his RTX-issued laptop, which contained ITAR-controlled technical data, to St. Petersburg, Russia and attempted to use the laptop while in Russia. Respondent reported that its cybersecurity team “first received an alert for the subject laptop on June 1, 2021, but incorrectly dismissed the alert and several subsequent alerts as a false positive” because Respondent was transitioning to a new cybersecurity tool and had “experienced a temporary increase in false positive geolocation alerts.” Respondent did not restrict the employee’s access to the RTX network until June 10, 2021, after which the employee returned to the United States.

Following the employee’s return from Russia, Respondent determined that the employee’s laptop hosted 152 files that contained USML Category VIII(i), XI(d), and XII(f) technical data, including SME, related to the F-15 Eagle Fighter Aircraft, F/A-18 Hornet Fighter Aircraft, the F-22 Raptor Fighter Aircraft, the F-35 Lightning II Fighter Aircraft, and the U-2 Reconnaissance Aircraft. Respondent also determined that the employee “had traveled to Russia on personal travel on four prior occasions since the start of his employment in July 2019 . . . to visit his fiancée” and that he had taken his RTX-issued laptop with him on at least one of these earlier trips.

Unauthorized Exports to Iran

In a 2019 disclosure, Respondent described the unauthorized export of defense articles to Iran, a proscribed destination listed in 22 C.F.R. 126.1, during one employee’s personal travel. In March 2019, Respondent’s employee hand-carried his company-issued laptop, which contained ITAR-controlled technical data, to Iran. Respondent detected the employee’s attempt to use the laptop to connect to the internet while in Iran and initiated a “freeze” in response, restricting access to the laptop’s hard drive. Following the employee’s return to the United States, Respondent determined that the laptop contained USML Category VIII(i) technical data related to the B-2 Spirit Bomber Aircraft and F-22 Raptor Fighter Aircraft.

IV. Violations of Terms, Conditions, and Provisos of DDTC Authorizations

Respondent has submitted 36 disclosures to the Department related to its violations of terms, conditions, and provisos of DDTC authorizations on numerous occasions dating back to 2019. These violations comprise:

- Failure to furnish or properly complete DSP-83 Nontransfer and Use Certificates;
- Failure to return in a timely manner to the United States defense articles previously exported under DSP-73 temporary export licenses;
- Failure to file or the filing of inaccurate annual sales reports related to Department-issued manufacturing licensing agreements (MLA);
- Failure to file in a timely manner reports related to payments reportable under 22 C.F.R. 130;
- Failure to notify DDTC in a timely manner of actions related to Department-issued authorizations (e.g., agreement termination, agreement execution, failure to conclude agreements, initial export of technical data pursuant to an agreement);
- Foreign manufacture of defense articles valued in excess of that authorized by the relevant MLA; and
- Misrepresentation or omission of facts in export or temporary import control documents (e.g., citation of incorrect Department-issued authorizations in electronic export information filings, submission of amendments to Department-issued MLAs containing inaccurate valuations of defense articles manufactured abroad).

The Department notes that Respondent submitted 14 of the abovementioned 36 voluntary disclosures during or prior to 2021, and in each disclosure included corrective actions intended to address the root causes of the disclosed violations and prevent their recurrence. Respondent continued to discover, and, in at least one case continued to commit, similar violations into 2023.

Further, in at least two cases, Respondent elected not to conduct a comprehensive review of its potential past violations of terms, conditions, and provisos of DDTC authorizations, instead reviewing authorizations that were “active” (i.e., not expired) at the time of the review. In response to the Department’s request to explain this decision, Respondent explained that it restricted its review to active authorizations because Respondent “determined that the ongoing risk of continued non-compliance was greatest with the authorizations still in use.” Respondent further explained that Respondent “[did] not intend to conduct a review of its [nearly 700] DSP-73 and DSP-61 authorizations that expired in the past five years” based on its “analysis on the potential risk posed by its expired authorizations” from the types of violations identified through the review of active licenses, and the “time and resources that [Respondent] anticipate[d] that a review of its expired DSP-73 and DSP-61 licenses would take.”

RELEVANT ITAR REQUIREMENTS

The relevant period for the alleged conduct is August 5, 2017, through September 29, 2023. The regulations effective as of the relevant period are described below. Any amendments to the regulations during the relevant period are identified in a footnote.

Part 121 of the ITAR identifies the items that are defense articles, technical data, and defense services pursuant to § 38 of the AECA.

Section 123.1(a) of the ITAR provides that any person who intends to export or to import temporarily a defense article must obtain the approval of the DDTC prior to the export or temporary import, unless the export or temporary import qualifies for an exemption under the provisions of this subchapter.

Section 126.1(a) of the ITAR provides that it is the policy of the United States to deny, among other things, licenses and other approvals for exports and imports of defense articles and defense services, destined for or originating in certain countries, including the PRC.

Section 127.1(a)(1) of the ITAR provides that is unlawful to export or attempt to export from the United States, any defense article or technical data, or to furnish any defense service for which a license or written approval is required by the ITAR without first obtaining the required license or written approval from DDTC.

Section 127.1(a)(2) of the ITAR provides that is unlawful to reexport or retransfer or attempt to reexport or retransfer any defense article, technical data, or defense service from one foreign end-user, end-use, or destination to another foreign end-user, end-use, or destination for which a license or written approval is required by the ITAR without first obtaining the required license or written approval from DDTC.

Section 127.1(b) of the ITAR provides that it is unlawful to violate any of the terms or conditions of a license or approval from DDTC, any exemption under the ITAR, or any rule or regulation contained in the ITAR.

Section 122.5 of the ITAR requires any person who is required to register to maintain records concerning the manufacture, acquisition, and disposition (to include copies of all documentation on exports using exemptions and applications

and licenses and their related documentation) of defense articles, technical data, and provision of defense services. Such records must be in an electronic format using a process or system capable of reproducing all records on paper. All records must be maintained for a period of five years from the date of the transaction. Such records must be available at all times for inspection and copying by the Directorate of Defense Trade Controls. Upon request, the person maintaining the records must furnish the records required to be maintained in accordance with the ITAR.

CHARGES

Charges 1-550: Unauthorized Exports, Reexports, Retransfers, and Temporary Imports Resulting from the Failure to Establish Proper Jurisdiction and Classification

Respondent violated 22 C.F.R. 127.1(a)(1) 222 times when it exported without authorization defense articles controlled under USML Categories VIII(h), VIII(i), XI(c), XI(d), and XII(f) to the PRC from 2017-2023.

Respondent violated 22 C.F.R. 127.1(a)(2) three times when it retransferred without authorization defense articles controlled under USML Category XI(d) within the PRC in 2021.

Respondent violated 22 C.F.R. 127.1(a)(1) 49 times when it exported without authorization defense articles related to sensitive military platforms controlled under USML Categories IV(h), VI(f), XI(c), and XI(d) to Australia, Canada, France, Germany, Greece, Japan, Mexico, the Netherlands, Saudi Arabia, Singapore, the UAE, and the United Kingdom from 2017 to 2022.

Respondent violated 22 C.F.R. 127.1(a)(1) 151 times when it exported without authorization defense articles, including SME, controlled under USML Categories IV(c), VI(f), VIII(g), VIII(h), VIII(i), XI(a), XI(c), XI(d), XII(e), XII(f), XIII(b), XIII(l), and XIX(g) to Argentina, Australia, Brazil, Canada, the Czech Republic, France, Germany, India, Indonesia, Israel, Italy, Japan, Malaysia, Mexico, the Netherlands, New Zealand, Pakistan, the Philippines, Poland, the Republic of Korea, Romania, Saudi Arabia, Singapore, Spain, Sweden, Taiwan, Thailand, Türkiye, the UAE, and the United Kingdom from 2017 to 2023.

Respondent violated 22 C.F.R. 127.1(a)(2) 87 times when it reexported without authorization defense articles, including SME, controlled under USML Categories VIII(h), XI(a), XI(c), and XI(d) to Bosnia and Herzegovina, the Czech Republic, Italy, Mexico, the Republic of Korea, Saudi Arabia, Spain, Sweden, and the UAE from 2018 to 2022.

Respondent violated 22 C.F.R. 127.1(a)(2) 12 times when it retransferred without authorization defense articles controlled under USML Categories VIII(h) and XI(c) within Germany and the United Kingdom from 2018 to 2022.

Respondent violated 22 C.F.R. 127.1(a)(3) 26 times when it temporarily imported without authorization defense articles controlled under USML Categories VIII(h) and XI(c) from Portugal and Taiwan from 2019 to 2022.

Charges 551-631: Unauthorized Exports, Reexports, and Retransfers of Defense Articles, including Classified Defense Articles

Respondent violated 22 C.F.R. 127.1(a)(1) five times when it exported without authorization classified defense articles controlled under USML Categories IV(h), IV(i), and XI(c) to Australia, Germany, Norway, and the UAE from 2019 to 2021.

Respondent violated 22 C.F.R. 127.1(a)(2) two times when it retransferred without authorization classified defense articles controlled under USML Categories II(k) and XII(f) within Canada in 2021 and 2022.

Respondent violated 22 C.F.R. 127.1(b)(1) four times when it exported classified defense articles controlled under USML Categories VII(h), XI(d), and XII(f) to Australia and Israel in violation of provisos to DDTC authorizations from 2019 to 2021.

Respondent violated 22 C.F.R. 127.1(a)(1) 53 times when it exported without authorization defense articles, including SME, controlled under USML Categories IV(i), VI(g), VIII(h), VIII(i), IX(b), XI(a), XI(c), XI(d), XII(c), XII(e), XII(f), XIX(f), and XIX(g) to Algeria, Canada, France, Germany, Greece, India, Indonesia, Israel, Japan, Luxembourg, Mexico, the Netherlands, Norway, Poland, the PRC, the Republic of Korea, Saudi Arabia, Singapore, Spain, Sweden, Türkiye, and the United Kingdom from 2017 to 2023.

Respondent violated 22 C.F.R. 127.1(a)(2) 13 times when it reexported without authorization defense articles, including SME, controlled under USML Categories XI(a), XI(c), XII(e), and XII(f) to India, the Philippines, the PRC, and Sweden from 2018 to 2022.

Respondent violated 22 C.F.R. 127.1(a)(2) four times when it retransferred without authorization defense articles, including SME, controlled under USML Categories VIII(i) and XI(a) within Poland and the United Kingdom in 2021 and 2022.

Charges 632-635: Unauthorized Exports of Defense Articles by Employees via Hand-Carry to Proscribed Destinations

Respondent violated 22 C.F.R. 127.1(a)(1) four times when it exported without authorization defense articles, including SME, controlled under USML Categories IV(i), VIII(i), XI(d), and XII(f) to Iran, Lebanon, and Russia from 2019 to 2021.

Charges 636-750: Violations of Terms, Conditions, and Provisos of DDTC Authorizations

Respondent violated 22 C.F.R. 127.1(b)(1) 96 times when it violated the terms, conditions, and provisos of DDTC authorizations from 2018 to 2023.

Respondent violated 22 C.F.R. 127.2(a) 18 times when it misrepresented or omitted facts for the purpose of exporting, transferring, reexporting, retransferring, obtaining, or furnishing defense articles from 2018 to 2023.

Respondent violated 22 C.F.R. 122.5(a) one time when it failed to maintain records concerning the manufacture, acquisition, or disposition of defense articles in 2021.

ADMINISTRATIVE PROCEEDINGS

Pursuant to 22 C.F.R. 128.3(a), administrative proceedings against a respondent are instituted by means of a charging letter for the purpose of obtaining an Order imposing civil administrative sanctions. The Order issued may include an appropriate period of debarment, which shall generally be for a period of three (3) years, but in any event will continue until an application for reinstatement is submitted and approved. Civil penalties, not to exceed \$1,238,892, per violation of

22 U.S.C. § 2778, may be imposed as well, in accordance with 22 U.S.C. § 2778(e) and 22 C.F.R. 127.10.

A respondent has certain rights in such proceedings as described in 22 C.F.R. Part 128. This is a proposed charging letter. In the event, however, that the Department serves Respondent with a charging letter, the company is advised of the following:

You are required to answer a charging letter within 30 days after service. If you fail to answer the charging letter, your failure to answer will be taken as an admission of the truth of the charges and you may be held in default. You are entitled to an oral hearing, if a written demand for one is filed with the answer, or within seven (7) days after service of the answer. You may, if so desired, be represented by counsel of your choosing.

Additionally, in the event that the company is served with a charging letter, its answer, written demand for oral hearing (if any), and supporting evidence required by 22 C.F.R. 128.5(b), shall be in duplicate and mailed to the administrative law judge designated by the Department to hear the case at the following address:

USCG, Office of Administrative Law Judges G-CJ,
2100 Second Street, SW
Room 6302
Washington, DC 20593

A copy shall be simultaneously mailed to the Deputy Assistant Secretary for Defense Trade Controls:

Deputy Assistant Secretary Michael Vaccaro
U.S. Department of State
PM/DDTC
SA-1, 12th Floor
2401 E Street, NW
Washington, DC 20522-0112

If a respondent does not demand an oral hearing, it must transmit within seven (7) days after the service of its answer, the original or photocopies of all correspondence, papers, records, affidavits, and other documentary or written evidence having any bearing upon or connection with the matters in issue.

Please be advised also that charging letters may be amended upon reasonable notice. Furthermore, pursuant to 22 C.F.R. 128.11, cases may be settled through consent agreements, including after service of a proposed charging letter.

The U.S. government is free to pursue civil, administrative, and/or criminal enforcement for AECA and ITAR violations. The Department of State's decision to pursue one type of enforcement action does not preclude it, or any other department or agency, from pursuing another type of enforcement action.

Sincerely,

Michael Vaccaro
Deputy Assistant Secretary
Bureau of Political-Military Affairs