Supply Chain Security, Privacy & Gov't Regulatory Compliance

Revised 09/15/23

This document will detail the specific supplier requirements for the Supply Chain Security, Privacy & Gov't Regulatory compliance program. Please read and understand the detail below, which will help explain what needs to be done and why.

There could be additional requirements throughout the year that are not fully comprehended or documented at this time. These could include additional government regulatory, assessment or audit requests, or actions required resulting from an audit/assessment, or any other requirement Intel deems necessary, due to a change in the risk landscape.

All suppliers providing hardware, developing software, managing systems and/or processing data on behalf of Intel must meet the minimum requirements outlined in the Intel Information Security Addendum (ISA) and as applicable in the **ISA Appendix A for Cloud Security,** or the **ISA Appendix B for Offshore Development Centers**. Intel suppliers are subject to Intel's data protection and cyber security requirements and all applicable laws, including all applicable data protection and cybersecurity laws and regulations.

Sub-Projects Included in this program:

1. Supply Chain Privacy Compliance Required for European Union (EU) and European Economic Area (EEA) Personal Data Transfers
2. Offshore Development Center Audits
3. Information Security Supplier Risk Assessment (RA)
4. SecurityScorecard™ Continuous Cyber Monitoring and Remediation
5. U.S. Government NDAA Section 889 and Section 5949 FAR 52.204-24 and FAR 52.204-25

1. Supply Chain Privacy Compliance Required for European Union (EU) and European Economic Area (EEA) Personal Data Transfers:

Step 1: Respond to email from **OneTrust** regarding the need to complete a **Transfer Impact Assessment - TIA.** (Approximately 80 questions)

Step2: Participate as requested in conversations with Intel Privacy Legal or Corporate Privacy to determine required supplementary controls.

Step 3: As applicable, implement supplemental controls identified by Intel Legal.

2. Offshore Development Center Audits (ODC)

Step 1: Acknowledge email or OneTrust request from Intel Information Security team to participate in an Audit. The Audit may be on-site, performed remotely or conducted by a third party on behalf of Intel.

Step 2: Ensure you are familiar with the Intel Information Security Addendum (ISA) and appendices pertaining to Information Security requirements for Cloud Security and ODCs. These can be found on Supplier.intel.com here:

Intel Information Security Addendum (ISA)

ISA Appendix A for Cloud Security

ISA Appendix B for Offshore Development Centers

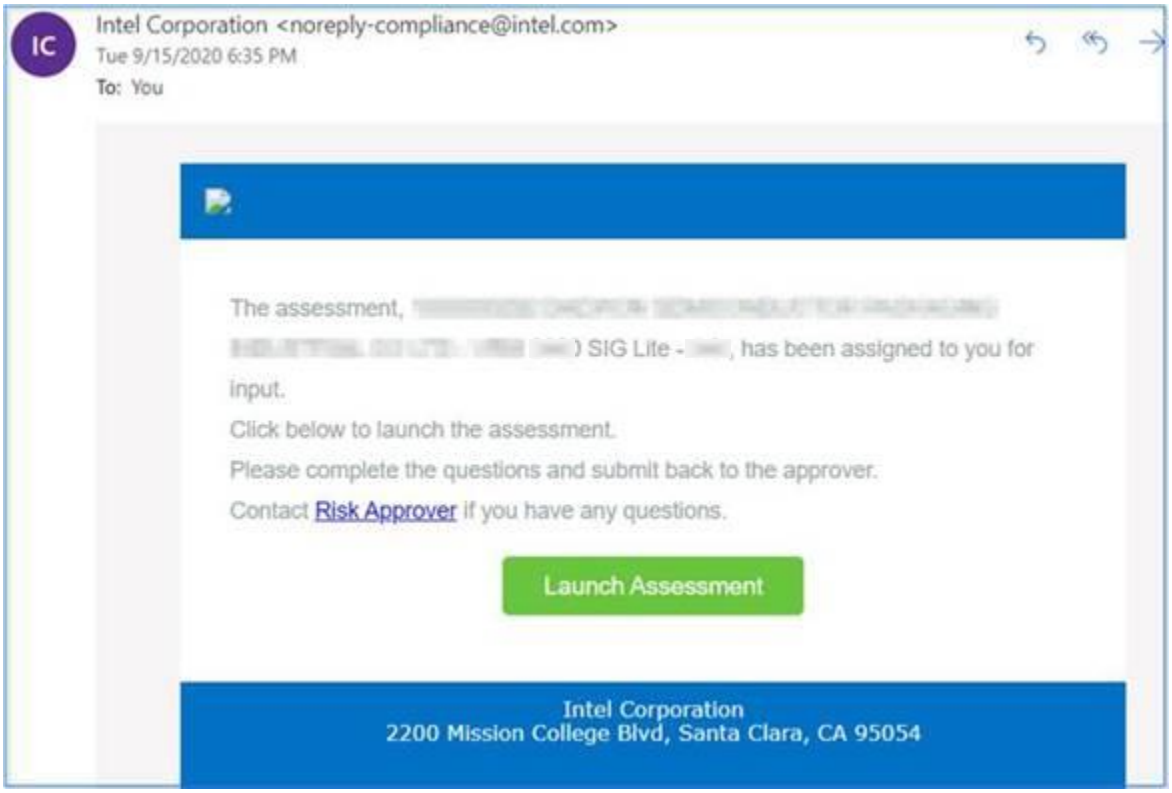
Step 3: Prepare for the audit as requested by Information Security. This may entail completing an online questionnaire or providing relevant industry attestations or certifications.

Step 4: Support the audit (on-site or remote) with prepared personnel.

Step 5: Acknowledge any remediation actions and complete actions per assigned deadline in the audit report.

3. Information Security Supplier Risk Assessment (RA)

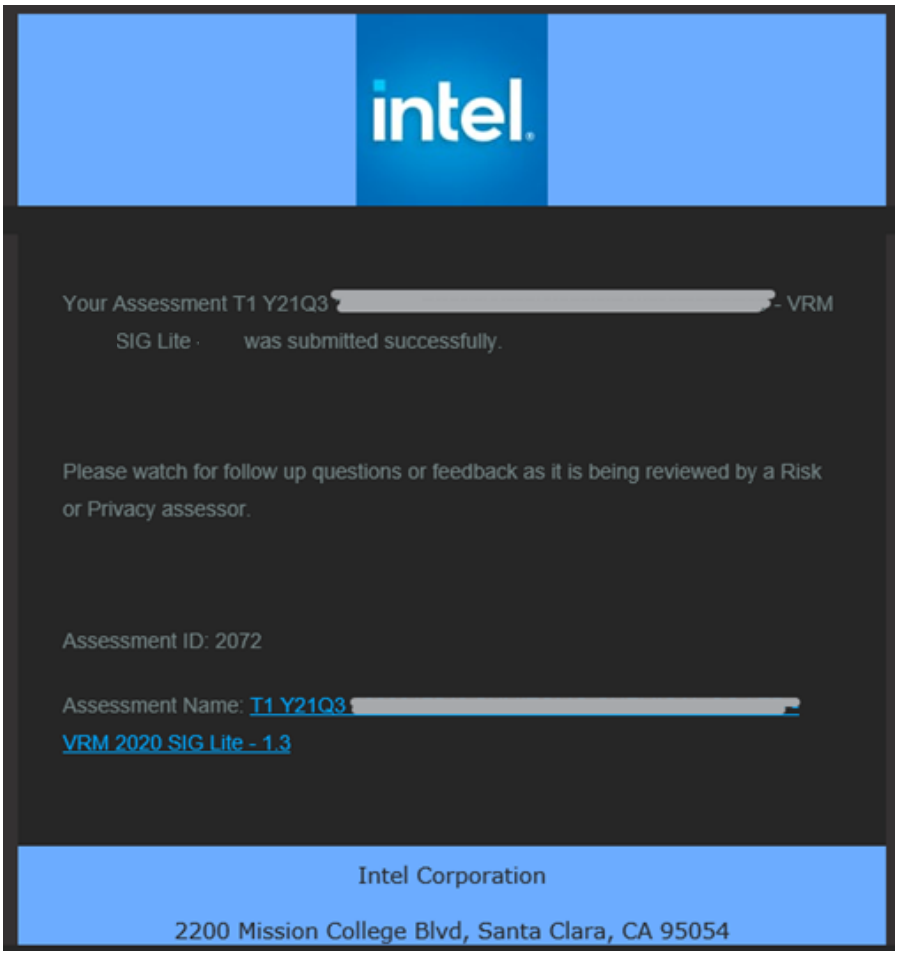
Step 1: Acknowledge OneTrust email request from Intel Information Security team to participate in a supplier Risk Assessment. The assessment will be conducted remotely and will require documentation to be provided.



Step 2: Provide all requested documentation which will include completing an industry standard SIG Lite questionnaire, in our online platform, as well as providing copies of relevant information security attestations, such as an ISO27001 certification. The assessment cannot move forward until ALL requested documentation is provided.

SIG Lite Workflow Diagram

You should see this message once the questionnaire is fully completed.



Step 3: Upon receipt of Assessment report, understand the risks that have been assigned and the assigned due date. The expectation is to meet the assigned due date unless not reasonably feasible. If a due date is not feasible, notify the Risk Assessor to negotiate a new deadline. Due dates are assigned based on the severity level of the vulnerability discovered.

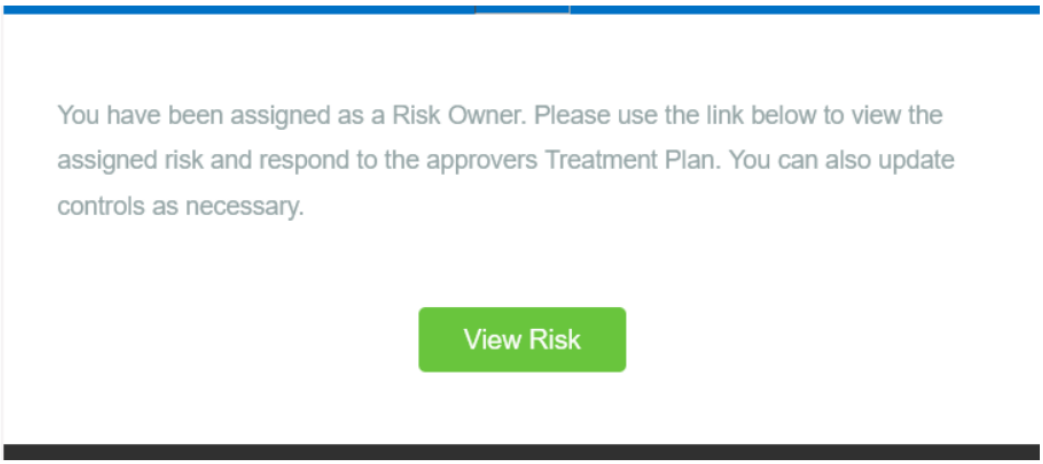
Step 4 : Complete remediation plans for all identified risks or findings from the assessment. Remediation actions will not be considered complete until required proof points are provided and status has been updated in OneTrust.

Detailed Description of How to Access Assigned Risks After an Assessment:

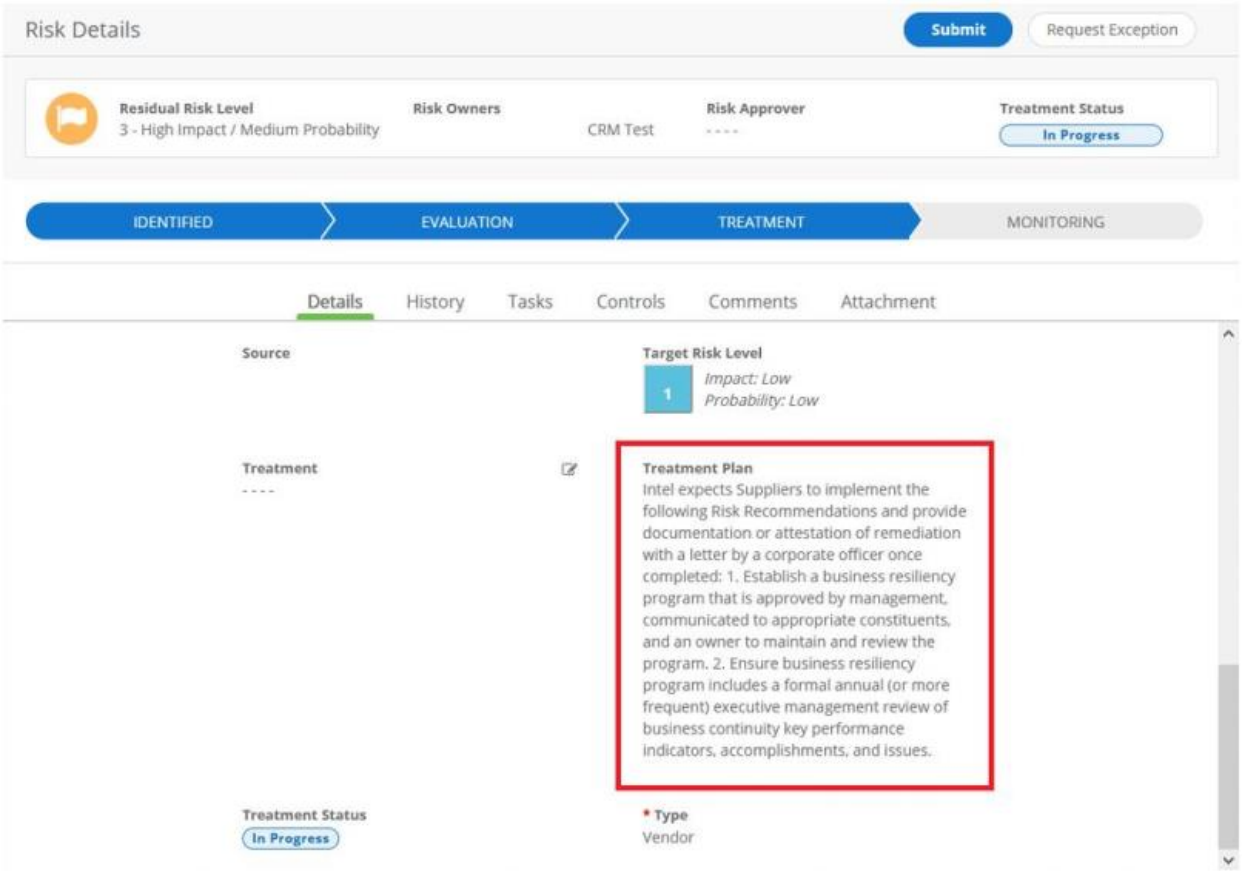
How to respond to a Risk as a Risk Owner

Follow these steps to access and respond to a Risk:

1. Click on **View Risk** in the email notifying that you have been assigned as a **Risk Owner**.

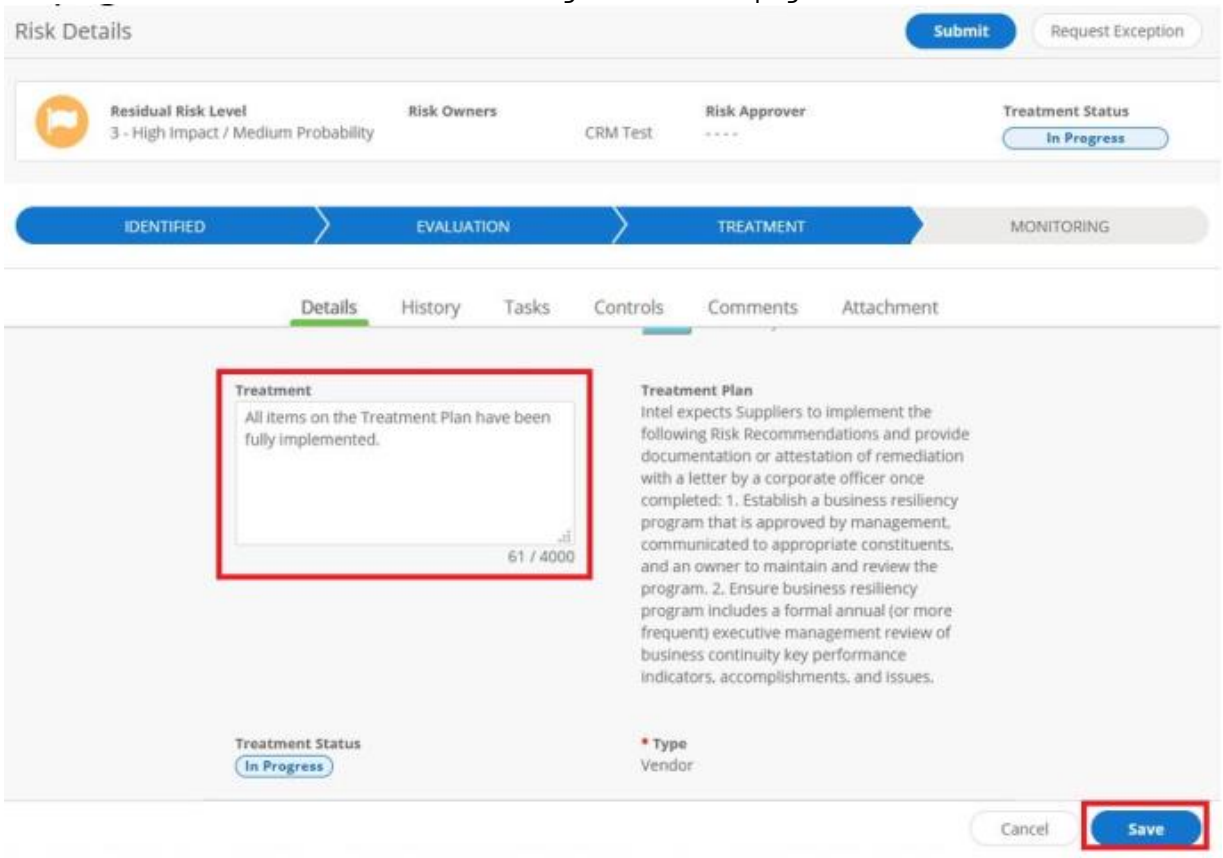


2. Review the recommended **Treatment Plan** and determine how and when the items listed can be implemented.

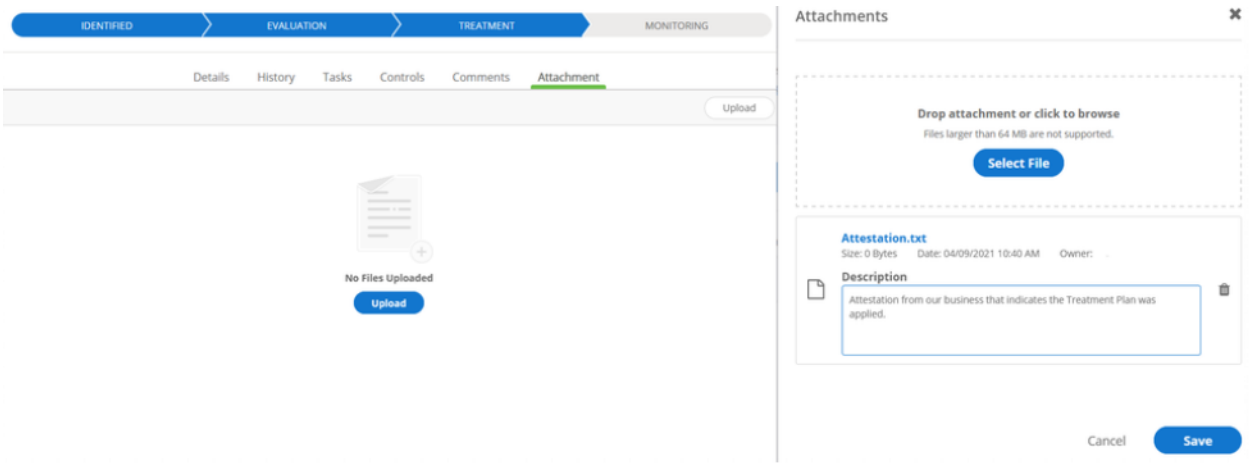


3. Hover over the **Treatment** field and click to bring up the text field.

4. In the **Treatment** field, provide details about what steps were taken to implement the **Treatment Plan** or address the **Risk** and click the **Save** button in the bottom right corner of the page.

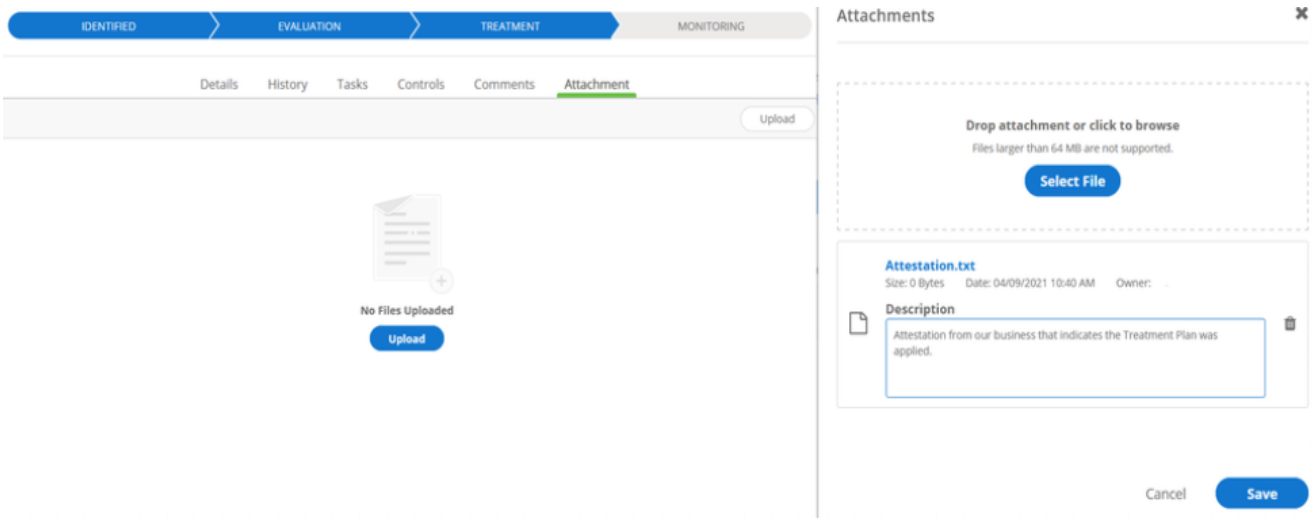


5. To attach any attestations of Treatment implementations, select **Attachment** and click **Upload** to attach a file to the Risk. Add a **Description** for the attachment and click **Save**.



6. Once the **Treatment** field has been updated and any necessary **attachments** have been uploaded, click the **Submit** button in the top right corner of the page. Enter any additional comments and click the **Submit** button to send the Risk to Cyber Risk Management for review.

   NOTE: Do NOT use the **Request Exception** button. This functionality is currently not supported by Intel Information Security and all requests for an exception will be denied and sent back to the **Risk Owners**. If **Risk Acceptance** is required, please provide details in the **Treatment** field that explain why the **Treatment Plan** cannot be implemented and use the **Submit** button to send it to Intel Information Security for further review.



4. SecurityScorecard™ Continuous Cyber Monitoring and Remediation

Step 1: Intel will send the supplier contact an invitation to SecurityScorecard™. Access is FREE to all Intel suppliers when invited by Intel, and you do NOT need to register annually.

Step 2: Accept the invite and register the account in SecurityScorecard™. Review and understand the vulnerabilities that have been flagged and contribute to the poor grade(s). Follow the FAQ for Invited Vendors or General Help Questions for more information.

Step 3: Address issue findings in the scorecard by following the instructions.

Step 4: Set up alerts by following the instructions for Notification Settings.

Step 5: Implement all required remediation actions suggested by SecurityScorecard™ so that the overall supplier grade is at least a "B" = "80" or better and monitor the scorecard regularly throughout the year to maintain a "B" or better.

Step 6: Review scorecard with Intel contact on a quarterly basis to ensure compliance.

5. U.S. Government NDAA Section 889 & Section 5949 FAR 52.204-24 and FAR 52.204-25

Intel Corporation, as a Federal Contractor, is required to maintain compliance to the U.S. Government NDAA Section 889 & Section 5949 throughout our supply chain. Intel Corporation and our global suppliers are prohibited from procuring or using, equipment, services and components as defined by these Federal Acquisition Regulations (FARs) and within the contracted scope of work the supplier has with Intel Corporation:

U.S. Federal Acquisition Regulation (FAR) 52.204-24, -25, and -26 48 CFR 52.204-24, -25, and -2626, which implements Section 889 of the 2019 National Defense Authorization Act and Section 5949 of the 2023 National Defense Authorization Act, prohibits Federal Contractors from providing to the U.S. Government any equipment, system, or service that uses "covered equipment or services" and "covered semiconductor parts or services" from eight Chinese companies, their subsidiaries and affiliates, as a substantial or essential component of any system, semiconductor part, product or service, or as critical technology as part of any system.

FAR 52.204-25(a) defines "covered telecommunications equipment or services" as:

- Equipment or services produced or provided by Huawei Technologies Company, ZTE Corporation, or their subsidiaries or affiliates;
- Video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or their subsidiaries or affiliates, if such equipment is used for public safety security of government facilities, physical security surveillance of critical infrastructure, or other national security purposes;
- Video surveillance or telecommunications services provided by such entities or using such equipment; or
- Telecommunications or video surveillance equipment or services produced or provided by any other entity that has been identified by the U.S. government as being subject to this provision
- Section 5949 of the FY 2023 NDAA amends Section 889 of the FY 2019 NDAA by expanding the current prohibition implemented at FAR 52.204-24, -25, and -26 to further prohibit procuring or obtaining any electronic parts, products, or services that include covered semiconductor parts or services as a semiconductor product or service that incorporates a semiconductor product that is designed, produced, or provided by Semiconductor Manufacturing International Corporation, ChangXin Memory Technologies, or Yangtze Memory Technologies Corp

Intel's Supplier Compliance Handbook prohibits contracting for certain telecommunications, video surveillance services or equipment, or semiconductor part, product, or service, in support of U.S. NDAA Section 889 and Section 5949.

Intel will send a Section 889 & Section 5949 attestation request directly to the supplier through a 3rd party from ComplianceSurvey@Intel.com. Questions in the attestation request will relate to compliance of the U.S. Federal Government NDAA Section 889 and Section 5949 of the U.S. NDAA FAR 52.204-24, -25 and -26 and all compliance requirements therein. The supplier will need to complete the questions and submit their response by the due date listed in the attestation invite.

Resources

Supplier Compliance Handbook:

Intel Information Security Addendum (ISA)

ISA Appendix A for Cloud Security

ISA Appendix B for Offshore Development Centers