Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cos. Face Uncertainty In Commerce Foreign Adversary Rules

By **Cortney Morgan and Grant Leach** (February 11, 2021, 6:22 PM EST)

Cortney Morgan

Grant Leach

On Jan. 19, the U.S. Department of Commerce published a long-awaited interim final rule to address the use of goods or services sourced from foreign adversaries in the U.S. supply chain for information communications technology and services, or ICTS, transactions.[1]

When the interim final rules take effect on March 20, they will enable the secretary of commerce to block any ICTS transaction involving goods or services designed, developed, manufactured, or supplied from foreign adversaries or companies organized in a foreign adversary country, conducting operations in a foreign adversary country, or otherwise subject to the direction or control of a foreign adversary.

These rules will have especially broad application, but Commerce has also indicated that it will continue to accept comments on the rules until March 22.

Commerce will also publish procedures for a safe harbor licensing program before March 22, and will then implement that licensing program sometime on or before May 19.

Therefore, concerned parties still have an opportunity to submit feedback on the ICTS rules and also have some remaining time to evaluate whether their transactions or activities might require licensing from Commerce.

Background

The ICTS rules are required under Executive Order No.13873,[2] which President Donald Trump issued on May 15, 2019, in order to prohibit the U.S. ICTS sector from using goods or services sourced from foreign adversaries in transactions with the potential to harm U.S. national security, U.S. critical infrastructure or the U.S. digital economy.

Commerce previously issued a proposed version of the ICTS rules in November 2019, and asked for public comments on those rules.[3] Those comments were originally due on Dec. 27, 2019, but Commerce then extended the comment period until Jan. 10, 2020.

Commerce has since considered those comments and made modifications to those previous proposed rules in order to arrive at the interim final ICTS rules that will take effect in their current form on March 22, but which are also subject to a comment period set to expire on that same date.

After that comment period expires, Commerce has committed to issue a subsequent final version of the ICTS Rules, in which Commerce will address additional comments received during this comment period.

What is the justification for the ICTS rules?

Trump's Executive Order No. 13873 observed:
[F]oreign adversaries are increasingly creating and exploiting vulnerabilities in [ICTS], which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people.

The Jan. 19 Federal Register notice explains:
Some foreign adversaries are known to exploit the sale of software and hardware to introduce vulnerabilities that can allow them to steal critical intellectual property, research results (e.g., health data), or government or financial information from users of the software or hardware.

Commerce also noted the "widespread use of some consumer devices, networked surveillance, cameras, drones, or interconnection via the internet of computing devices embedded in every day objects" that provide foreign adversaries with the opportunity to collect swaths of sensitive personal data that they could use to conduct corporate espionage, or compile information for blackmailing purposes.

What types of transactions are subject to the ICTS rules?

The ICTS rules define an ICTS transaction as:
any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download.

However, the ICTS rules limit the Commerce secretary's blocking authority to only the following specific types of ICTS transactions:

- ICTS transactions in any of the 16 sectors identified in Presidential Policy Directive 21 on critical infrastructure security and resilience, including:
    - Chemicals;
    - Commercial facilities;
    - Communications;
    - Critical manufacturing:
    - Dams;
    - Defense industrial base;
    - Emergency services;
    - Energy;
    - Financial services;

    - Food and agriculture;
    - Government facilities;
    - Health care and public health;
    - Information technology;
    - Nuclear reactors;
    - Materials and waste;
    - Transportation systems; and
    - Water and wastewater systems.

- ICTS transactions involving a wide variety of specifically identified software, hardware and other products or services integral to data networks and data transmission systems;

- ICTS transactions involving products or services for the use, process or retention of sensitive personal data on greater than 1 million U.S. persons, including:

    - Financial data that could indicate an individual's financial distress or hardship;

    - Consumer credit reporting data;

    - Data sets used in various insurance applications;

    - Data relating to an individual's physical, mental or psychological health condition;

    - Private electronic communications such as e-mail, messaging or chat communications;

    - Geolocation data;

    - Biometric enrollment data including facial, voice, retina/iris and palm/fingerprint templates;

    - Data used for issuing government identification cards;

    - Data concerning U.S. government security clearances; and

    - Genetic information.

- ICTS transactions involving internet-enabled sensors, webcams and any other end-point surveillance or monitoring device, home networking devices, and drones and other unmanned aerial systems if greater than 1 million units have been sold to U.S. persons;

- ICTS transactions involving software designed primarily for internet communications such as desktop applications, mobile applications, gaming applications and web-based applications if they are in use by over 1 million U.S. persons; and

- ICTS transactions involving artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems or advanced robotics.

The ICTS rules specifically exempt ICTS transactions that have been authorized under a U.S. government-industrial security program.

Also exempt are transactions that are under active review or have been reviewed by the Committee on Foreign Investment in the United States in connection with the foreign acquisition of a U.S. business or U.S. real estate.

However, that CFIUS exemption is not available if the ICTS transaction is distinct from or subsequent to the CFIUS-reviewed transaction.

Who are foreign adversaries and persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary?

Commerce has identified China (including Hong Kong), Cuba, Iran, North Korea and Russia as foreign-adversary countries and has also identified acting Venezuelan president Nicolas Maduro individually as a foreign adversary.

The ICTS rules define a person owned by, controlled by or subject to the jurisdiction of a foreign adversary as:

- Any person, who acts as an agent, representative, or employee, or any person otherwise acting at the order, request, or under the direction or control of a foreign adversary;
- Any person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;
- Any person, wherever located, who is a citizen or resident of a nation-state controlled by a foreign adversary;
- Any business entity organized under the laws of a nation-state controlled by a foreign adversary; and
- Any business entity, wherever located, that is owned or controlled by a foreign adversary.

As discussed below, this definition will extend the ICTS rules' coverage to many information communications technology and services industry supply chains.

What types of transactions or activities are likely to be blocked or restricted under the ICTS rules?

The following factors may determine whether an ICTS transaction involves information communications technology and services designed, developed, manufactured or supplied by a person owned by, controlled by or subject to the jurisdiction of a foreign adversary, which will potentially subject the transaction to blocking under the ICTS rules:

- Whether the person or its suppliers have headquarters, research, development, manufacturing, test, distribution, service facilities or other operations in a foreign country, including one controlled by, or subject to the jurisdiction of, a foreign adversary;
- Whether any ties exist between that person and a foreign adversary. For business entities, this includes ties between their officers, directors, employees, consultants or contractors and a business entity;

- Laws and regulations of any foreign adversary country in which a person is headquartered or conducts operations, including research and development, manufacturing, packaging and distribution; and

- Any other criteria that the secretary of Commerce deems appropriate.

As a result, transactions or activities involving suppliers that are domiciled in what would otherwise be considered friendly countries could still be subject to the ICTS rules if those suppliers or their personnel have operations in or other connections to foreign adversary countries.

However, even if an ICTS transaction meets the above criteria, the rules also require that the transaction must present an undue or unacceptable risk before the secretary will be entitled to block the transaction.

The ICTS rules and the securing the ICTS supply chain executive order define an undue or unacceptable risk as (1) an undue risk of sabotage or subversion of the U.S. ICTS sector; (2) an undue risk of catastrophic effects on the security or resiliency of U.S. critical infrastructure or the U.S. digital economy; or (3) an unacceptable risk to U.S. national security or the security and safety of U.S. persons.

The ICTS rules require the secretary to consider seven specific factors when considering whether a transaction presents an undue or unacceptable risk.

Those factors include threat assessments issued by agencies such as the Office of the Director of National Intelligence, the U.S. Department of Homeland Security and the U.S. Department of Defense, and a general consideration of "the nature, degree, and likelihood of consequence to the United States public and private sectors that could occur if ICTS vulnerabilities were to be exploited."

What process will the secretary use for applying the ICTS rules?

The secretary's review process under the ICTS rules consists of a referral, an initial review, a first interagency consultation, an initial determination, a second interagency consultation and a final determination.

At various points in this process the secretary may abandon its review of a transaction, but will retain the right to conduct further review if additional information becomes available. Certain stages require that the secretary consult with appropriate federal agency or department heads that the secretary may determine to be appropriate.[4]

Throughout the review process the secretary also enjoys broad authority to seek additional information from transaction parties. The ICTS rules require transaction parties to comply with any such request.

The ICTS rules give the secretary and appropriate agency heads a great deal of discretion in deciding how they want to administer this review process, which could create significant uncertainty for the ICTS industry.

It appears that the referral, initial review and first interagency consultation stages will have the potential to blur together in practice.

During those stages, the ICTS rules do not require Commerce to provide companies with any notice that

their transactions are under review. Instead, transaction parties are only entitled to receive notice if the review advances beyond the first interagency consultation and results in an initial determination by the secretary and the appropriate agency heads that the transaction presents an undue or unacceptable risk.

In that instance, the secretary will issue an initial written determination explaining why the transaction is subject to the ICTS rules and setting forth the initial determination, either to prohibit the transaction or require that the parties adopt mitigation measures in order to continue with the transaction.

The secretary may notify the parties to the transaction of this initial determination either by serving them a copy privately or by publishing it in the Federal Register.

After the secretary serves an initial determination notice, the parties to an affected transaction have 30 days to protest the secretary's determination or propose alternative remedial measures.

If the parties submit a response, the secretary shall then conduct a second interagency consultation with the appropriate agency heads and attempt to reach a consensus as to whether the transaction should be prohibited, permitted or permitted only pursuant to the adoption of negotiated mitigation measures.

If the secretary and the appropriate agency heads reach a consensus decision, then they will issue that decision as a final determination.

If they cannot reach a consensus, then the secretary will refer the transaction to the president, and will issue a final determination according to direction received from the president.

All final determinations will be sent to the transaction participants, and if the final determination results in a decision to prohibit the transaction then the secretary will also publish a summary of the final determination result in the Federal Register with any confidential business information omitted.

This could result in a situation that would require companies in the ICTS industry to proactively monitor the Federal Register in order to make themselves aware of any hardware, software or services that may become blocked under the ICTS Rules.

To the extent that a reviewed transaction will warrant a final determination, the ICTS rules require the secretary to issue that final determination within 180 days of commencing its initial review of the transaction. However, the secretary may unilaterally extend that deadline by making a written determination that additional time is necessary.

How will the licensing program function under the ICTS rules?

Commerce intends to offer a process whereby it will issue licenses for proposed, pending or ongoing ICTS transactions that are consistent with U.S. national security.

Congress intends to publish these licensing procedures by March 22 — the first business day occurring 60 days after the Federal Register notice — and to begin administering the licensing program and accepting license applications no later than May 19 — the date occurring 120 days after the Federal Register notice.

Commerce has announced that it will administer this licensing program on a fixed timeline and will issue

licensing decisions within 120 days after accepting a license application. If Commerce does not issue a license decision within that 120-day period, then the application will be deemed granted.

Interested parties should be aware that Commerce has a history of missing the deadlines in the executive order. The order originally required Commerce to publish the ICTS rules no later than Oct. 14, 2019, and this most recent Commerce ICTS rules announcement arrived 463 days past that initial deadline.

Therefore, if past practices are any indication, some of the ICTS rules' cutoff dates should be viewed as optimistic targets rather than hard-and-fast deadlines.

Are the ICTS rules likely to change now that the Biden administration has assumed office?

Commerce published the ICTS rules on Trump's final full day in office. When President Joe Biden took office the next day, one of his very first actions was to issue a regulatory freeze.[5]

For rules such as the ICTS rules that were published in the Federal Register but that have not yet taken effect, the regulatory freeze asked issuing agency to consider postponing their effective dates for 60 days, and to also consider opening a 30-day comment period in order to allow the Biden administration additional time to review any questions of fact, law and policy raised by the rules.

As discussed above, the ICTS rules already comply with the regulatory freeze because they were issued with a 60-day delay in their effective date and with a 60-day comment period — subject to a 1-day timing discrepancy due to differences between the publication date of the ICTS rules and the regulatory freeze.

We therefore expect that the Biden administration will use the next 60 days to consider the ICTS rules. Because the ICTS rules are authorized under Trump's executive order, Biden could theoretically revoke the order at any time during that review and thereby also invalidate the ICTS rules.

However, the rules are consistent with several national security initiatives that predate the Trump administration and we therefore believe it is unlikely that Biden will completely revoke the ICTS rules.

Instead, if the Biden administration does object to the ICTS rules, we believe that it is much more likely to address those concerns through the forthcoming licensing process, or through modifications to the ICTS rules that could be made after the final comment period concludes.

Alternatively, because the ICTS rules' transaction review process will largely take place outside of the public view, the Biden administration could choose to leave the ICTS rules intact, while implementing its desired policy objectives behind the scenes through enforcement directives issued to Commerce and the other appropriate agency heads.

Considering Commerce's past delays in implementing these rules and the ICTS rules' short turnaround times for concluding the comment period and establishing the required licensing program, it's also possible that the Biden Administration could take limited action to delay the ICTS rules' effective date or to extend some of their deadlines in order for Biden's new appointees at Commerce to further consider the ICTS rules' more substantive provisions.

What should I be doing to prepare for these rules?

If companies have specific concerns about the ICTS rules, then they should consider submitting a comment before the comment period expires on March 20.

Otherwise, companies engaged in the specific types of transactions that are covered by the ICTS rules should begin reviewing their supply chains to determine whether any of their suppliers — or their suppliers' suppliers — might qualify as "persons owned by, controlled by or subject to the jurisdiction or direction of a foreign adversary."

Although there is still significant uncertainty around the final form that the ICTS rules will eventually take and how Commerce will enforce them, companies can at least give themselves a head start by analyzing whether and to what extent the current ICTS rules might apply to them, and whether vendors in their ICTS supply chain might trigger blocking under the current version of the ICTS rules.

By proactively identifying those affected transactions and vendors, companies will be in a better position to apply for licenses, if appropriate, or to adjust their ICTS supply chain, if necessary.

Cortney Morgan and Grant Leach are partners at Husch Blackwell LLP.

[1] https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain.

[2] https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

[3] https://www.govinfo.gov/content/pkg/FR-2019-11-27/pdf/2019-25554.pdf.

[4] Examples include the secretary of the Treasury, secretary of Defense, secretary of the U.S. Department of State, U.S. Attorney General, secretary of Homeland Security, U.S. trade representative, Director of National Intelligence, administrator of the General Services Administration, chairman of the Federal Communications Commission.

[5] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/regulatory-freeze-pending-review/.