BILLING CODE 3510-33-P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

[Docket No. 200710-0186]

RIN 0694-XC063

Advanced Surveillance Systems and other Items of Human Rights Concern

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Notice of Inquiry.

SUMMARY: In this notice, the Department of Commerce (Department), Bureau of Industry and Security (BIS) seeks public comments on the list of items on the Export Administration Regulations' (EAR) Commerce Control List (CCL) that are controlled for crime control and detection (CC) reasons to promote human rights throughout the world. The request for comments in this notice furthers the periodic review of items controlled for CC reasons and is intended to inform the agency's decisions in updating (including additions and removals) items controlled for CC reasons on the CCL, as well as the related licensing requirements for such items. BIS takes this action pursuant to the Export Control Reform Act of 2018 (ECRA).

DATES: Comments must be received no later than **[INSERT 60 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER]**

ADDRESSES: Comments may be submitted by any of the following methods.

- *Federal rulemaking portal: http://www.regulations.gov* – you can find this notice by searching on its *regulations.gov* docket number, which is BIS– 2020–0021. All comments (including any personally identifying information) will be made available for public inspection and copying.

- By mail or delivery to Regulatory Policy Division, Bureau of Industry and Security, U.S. Department of Commerce, Room 2099B, 14th Street and Pennsylvania Avenue, NW, Washington, DC 20230. Refer to RIN 0694-XC056.

FOR FURTHER INFORMATION CONTACT: For questions on licensing requirements for items controlled for crime control reasons, contact Steven Schrader, Foreign Policy Division, Office of Nonproliferation and Treaty Compliance, Bureau of Industry and Security, U.S. Department of Commerce, by email at Foreign.Policy@bis.doc.gov, and by phone at 202-482-4252. For questions on the submission of comments, contact Sheila Quarterman, Regulatory Policy Division, Office of Exporter Services, Bureau of Industry and Security, U.S. Department of Commerce, by email at RPD2@bis.doc.gov .

SUPPLEMENTARY INFORMATION:

Background

The Bureau of Industry and Security (BIS) controls the export and reexport of items for crime control and detection (CC) reasons under the Export Administration Regulations (EAR) (15 CFR 730 – 774). The licensing requirements and policy for these items are set out in § 742.7 – Crime control and detection – of the EAR. These items are identified on the EAR's Commerce Control List (CCL) in Supplement No. 1 to Part 774 of the EAR.

BIS controls CC items to carry out the foreign policy of the United States, including to promote human rights throughout the world. The request for comments in this notice furthers the periodic review of items controlled for CC reasons and is intended to inform the agency's decision on updates (including additions and removals) of items listed on the CCL and controlled for CC reasons. BIS's last comprehensive review of CC items occurred with the assistance of comments submitted in response to a notice published in 2008 (73 FR 14769; March 19, 2008).

CC items of particular interest for new license requirements by BIS include facial recognition software and other biometric systems for surveillance, non-lethal visual disruption lasers, and long-range acoustic devices and their components, software, and technologies. BIS also seeks comments on the merits of removing or modifying the CC controls on several additional items currently on the CCL, and on potential controls for such items that are end-use/end-user based.

Request for Comments

BIS seeks comments from the public; including industry and trade organizations, non-governmental organizations, government agencies, and academia, on crime control and detection items of particular interest for new license requirements, including facial recognition software and other biometric systems for surveillance; non-lethal visual disruption lasers; and long-range acoustic devices and their components, software, and technologies.

BIS also seeks comments on current and proposed changes to items controlled on the CCL for CC reasons and on items designated as EAR99 on the CCL, including both the items noted below and related items.

1. Facial recognition software and other biometric systems
2. Non-lethal visual disruption lasers ("dazzlers")
3. Long-range acoustic devices and related components, software, and technologies for the above items.
4. Police helmets - 0A979
5. Fingerprint readers - 3A981, and components – (3A981, 4A980), software (3D980, 4D980), and technology (3E980, 4A980) thereof
6. Fingerprint powders, dyes, and inks (1A985)

7. Voice print identification systems (3A980) and components (3A980), software (3D980), and technology (3E980) thereof
8. Polygraphs and psychological stress analysis equipment (3A981) and components (3A981), software (3D980), and technology (3E980) thereof
9. Nonmilitary mobile crime science laboratories (9A980)
10. Miscellaneous CC controls in ECCNs and sub-paragraphs of ECCNs 4A003, 4A980, 4D001, 4D980, 4E001, 4E980, 6A002, 6E001, and 6E002

With regard to the aforementioned items described in more detail later in this notice, BIS seeks input on: 1) information (including performance criteria) that may distinguish purely or predominantly consumer or commercial applications from applications purely or predominantly for use by law enforcement or security services and/or used in mass surveillance, censorship, privacy violations or otherwise useful in committing human rights abuses; 2) the impact of adding to, modifying, or removing items from the CCL on U.S. support of human rights throughout the world; and 3) the impact that changes of controls would have upon the competitiveness of U.S. business and industry.

In addition to comments on the items listed below, BIS welcomes comments on the update of controls on other items for surveillance and crowd control as well as on related issues of concern to the public.

BIS also seeks comments on potential revisions to CC controls that are based on end-uses and/or end-users, such as the end-use/end-user controls in Part 744 of the EAR.

1. **Facial recognition devices for individuals or for crowd scanning, other biometric systems, and their input components, software, and technology**

A facial recognition system identifies or verifies a person's identity from a digital image or a video frame by comparing selected facial features from an input image to the features of faces stored in a database. The major components of a facial recognition system are (1) input camera(s), (2) data storage, (3) processing computer, and (4) the software algorithms needed to model facial images. While conventional facial recognition systems currently use cameras that see visible light, thermal imaging cameras that use infrared light are starting to be used in facial recognition systems due to their ability to operate independently of weather or lighting conditions.

Facial recognition is typically used to authenticate access to a device, such as on a cellphone, and is also widely used for access control into restricted areas, such as industrial facilities. Facial recognition systems have widespread user acceptance due to their contactless and non-invasive process.

Facial recognition is also increasingly used in crowd-scanning systems. Such systems are used in casinos (for tracking the location of employees, special customers, and barred customers), airports (for tracking staff and criminals), prisons (for tracking staff and inmates), customs facilities, and commercial facilities. Recently, such systems have also become popular as commercial customer/client identification and marketing tools. The systems also have utility to assist during Amber and Silver Alerts, to identify individual protestors in a crowd, including riot participants, or to track down escaped criminals, bail jumpers, and people with outstanding arrest warrants.

In addition to law enforcement and public safety-related uses, crowd-scanning systems can also be used to facilitate the abuse of human rights. China, for example, has deployed facial recognition technology in the Xinjiang region, in which there has been repression, mass arbitrary

detention and high technology surveillance against Uighurs, Kazakhs and other members of Muslim minority groups. Reporters visiting the region found surveillance cameras installed approximately every hundred meters in several cities, as well as facial recognition checkpoints at areas including gas stations, shopping centers, and mosque entrances.

BIS seeks input in particular on the high-resolution cameras currently classified as EAR99 on the CCL. Specifically the cameras' utility as inputs to crowd surveillance systems, and the implications of placing them under new controls is of interest to BIS: What specific technical criteria, such as resolution or framerate, would be appropriate for control; what criteria would differentiate these items as more compatible with police and intelligence end uses rather than with purely commercial end uses; and what impact would controls have upon U.S. industry competitiveness and leadership?

Other biometric controls

BIS also seeks information on controls for additional emerging biometric systems. Two methodologies of biometrics are currently controlled on the CCL: fingerprint and voice print. BIS seeks input on whether other biometric technologies merit control, and if so, what specific technical criteria would be appropriate to control, and what impact would controls have upon U.S. industry competitiveness and leadership.

As an alternative to piecemeal review of biometric methods and products, BIS could extend controls to all biometric systems – iris, vein, earlobe, gait, heartbeat, etc. – and then limit controls to only those types of systems that identify a person without the individual's cooperation, conscious interaction or possibly even awareness (e.g., a closed circuit camera running facial recognition software or surreptitious audio monitoring of a public space). Controls would not apply to systems that control access to premises or devices by verifying that

the person attempting to gain such access is authorized to do so. This approach would not control specific applications of the fingerprint, iris, and voice authentication commercial items. This type of control would capture potential technologies if they become mature. Because complete systems, software and technology are often the only essential items in facial recognition, EAR99 "parts" could remain excluded from controls, enhancing the ability to service exports otherwise authorized with no license required, under license exceptions, or by individual licenses. BIS seeks input on whether this approach would be better than targeting individual modalities, and if so, what specific technical criteria would be appropriate, and what impact controls would have upon U.S. industry and competitiveness.

2. Non-lethal visual disruption lasers ("dazzlers")

A dazzler is a non-lethal weapon which uses a laser to illuminate and temporarily disable sensors or human vision with flash blindness. Initially developed for military use, non-military products are becoming available for use in law enforcement and security. Dazzlers that emit infrared or invisible light against various electronic sensors, and visible light against humans. They are about the size of a flashlight, and can be hand-held or mounted to a small-arm weapon. Dazzlers are used for target acquisition, illumination, disorientation of human targets, and defeat of hostile sensor systems. Similar to common lasers, they can be used to maliciously disrupt civil and military aircraft operations by blinding a pilot or sensor system, potentially inducing a crash.

BIS could determine to control dazzlers under existing ECCN 0A504, which include controls on laser aiming devices or laser illuminators "specially designed" for use on firearms, and serve similar purposes. Control under this ECCN would impose CC1 requirements while

excluding Firearms Convention (FC1) requirements, which would allow their export to Canada license-free, in parallel with current aiming lasers for firearms.

3. Long-range acoustic devices (LRAD)

The Long-Range Acoustic Device (LRAD) is an acoustic hailing device used to send messages and warning tones over longer distances or at higher volume than normal loudspeakers. LRAD systems are used as a means of non-lethal, non-kinetic crowd control. They can be handheld, mounted on riot shields, or on vehicles. As an area denial device, the utility of such systems can be compared to tear gas, without the need for deploying forces to don protective equipment and minimizing collateral harm from shifting wind or canisters being thrown back.

LRAD systems are used by law enforcement, government and defense agencies, as well as by maritime and commercial security companies to broadcast audible notifications and warnings. LRAD systems are also used to deter wildlife from airport runways, wind and solar farms, nuclear power facilities, gas and oil platforms, mining and agricultural operations, and industrial plants. Additionally, LRAD systems can be used to conduct area denial operations. BIS also seeks public comment on ECCNS currently controlled on the CCL including:

4. Police helmets - 0A979

Police helmets are controlled under Export Control Classification Number (ECCN) 0A979, "Police helmets and shields; and "specially designed" "components," n.e.s." They are used for mounted duty (motorcycle, bicycle or horse) and occasionally for riot control purposes. However, most police agencies use helmets with ballistic protection controlled under ECCN 1A613.

5. Fingerprint readers - 3A981, and their components - 3A981, 4A980, software - 3D980, 4D980, technology - 3E980, 4A980

ECCN 3A981 controls, among other items, fingerprint analyzers, cameras and equipment, automated fingerprint and identification retrieval systems, and the "specially designed" "components" and "accessories" for them. Related hardware, software, and technology is controlled under ECCNs 3D980 and 4D980. Application specific software that is used by the operator, however, is designated as EAR99, because it doesn't meet all six criteria for the definition of "use" in EAR part 772: operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing.

Fingerprint-related items are used for device login authentication, area access controls, and identity verification for many private and public civil uses, as well as law enforcement uses. "Live scan" fingerprinting refers to both the technique and the technology used to capture fingerprints and palm prints electronically, without the need for the more traditional method of ink and paper. This is the predominant type of system currently in use, owing to the establishment of cross-platform standards promulgated by the National Institute of Science and Technology.

6. Fingerprint powders, dyes, and inks - 1A985

Fingerprint powders are used by crime scene investigators and others in law enforcement to obtain fingerprints and identify individuals at a particular scene or establish contact with a particular item. They may be employed by police or other authorities to identify individuals who wish to conceal their identity or to identify people who are incapacitated or deceased and thus unable to identify themselves. Their end use is almost entirely related to police forensics.

In contrast, fingerprint dyes and ink are employed in controlled but often voluntary situations, such as when a person hired for a sensitive position, is enrolled in a government benefit program (in some countries), or for identification documentation purposes. An

alternative to fingerprint dyes and inks are the live scan fingerprint capture devices controlled under ECCN 3A981, which are generally more effective, and in extensive use worldwide.

7. Voice print identification systems - 3A980, and their components - 3A980, software - 3D980, and technology - 3E980

Voice print identification systems are used to verify the identity of a speaker as part of a security process (1:1 matching) or for identification of an unknown speaker among a set of known speakers (1:n matching). Speaker verification is usually employed as a "gatekeeper" methodology prior to providing access to a secure system. Gatekeeper systems operate with the users' knowledge and typically require their cooperation. However, when voice print identification systems are used for identification, as compared to verification, systems can be implemented without the speaker's or speakers' knowledge to identify discussion participants, provided sufficient voice samples are in the searcher's database.

Voice print identification is used by private companies, especially by financial institutions, for telephonically-based customer service activities to identify clients, in both the private and government sectors to verify identities for user access to resources, services, or facilities, and in criminal investigations to identify persons of interest.

8. Polygraphs and psychological stress analysis equipment - 3A981, and their components - 3A981, software - 3D980, and technology - 3E980

A polygraph is a device that measures and records several physiological indicators such as blood pressure, pulse, respiration, and skin conductivity while a person is asked and answers a series of questions. The basis underpinning the use of the polygraph and other stress analysis equipment is that deceptive answers will produce physiological responses that can be differentiated from those associated with non-deceptive answers. Polygraphs are used in the

United States to much greater extent than most other countries, predominantly in law enforcement but also in the private sector to screen prospective employees or during misconduct investigations.

The current market for non-polygraph psychological stress analysis is almost entirely dominated by voice stress analysis (VSA) or computer voice stress analysis (CVSA). VSA is a technology that aims to infer deception from stress measured in the voice. CVSA records the human voice using a microphone and is based on the tenet that the non-verbal, low-frequency content of the voice conveys information about the physiological and psychological state of the speaker. Typically utilized in investigative settings, both VSA and CVSA aim to differentiate between stressed and non-stressed outputs in response to questions, with high stress seen as an indication of deception.

9. Nonmilitary mobile crime science laboratories - 9A980

To meet the standards of the items controlled under ECCN 9A980, mobile crime lab vehicles must contain one or more analytical or laboratory items controlled for CC reasons on the CCL, such those controlled under as ECCNs 3A980 and 3A981. Mobile crime labs provide on-site, rapid, reliable analysis of unknown compounds and materials for forensic, homeland security and military applications. They enable crime-scene technicians to conduct extensive evidence collection and processing at crime-scene sites, such as homicide scenes, methamphetamine lab and arson sites, and investigations that involve mass casualties. Most mobile crime labs contain equipment for analyzing chemicals, special hoods for fume disposal, isolated boxes for hazardous material analysis, and supplies for crime-scene investigation.

While the equipment in mobile crime labs is predominantly EAR99, as noted above, to qualify for control under ECCN 9A980, the lab must have one item controlled for CC reasons on

the CCL. For example, a lab could contain the fingerprint readers and polygraphs controlled under ECCN 3A981, the fingerprint powder, dyes, and ink controlled under 1A985, ancillary police equipment controlled for CC or FC reasons, and or instruments and chemicals controlled on the CCL for antiterrorism reasons, such as 2A994 portable electric generators. Additionally, some items stocked in a mobile crime lab could have higher controls, such as the personal protective equipment controlled under ECCN 1A613.

10. Miscellaneous CC controls in ECCNs and sub-paragraphs of ECCNs 4A003, 4A980, 4D001, 4D980, 4E001, 4E980, 6A002, 6E001, 6E002

a.) 4A003: "Digital computers", "electronic assemblies", and related equipment therefor, as follows (see List of Items Controlled) and "specially designed" "components" therefor. Within this entry, the items are controlled for CC are "digital computers" for computerized finger-print equipment.

b.) 4A980: Computers for fingerprint equipment, n.e.s. The entry for ECCN 4A980 does not control equipment limited to one finger and designed for user authentication or access control.

c.) 4D001: "Software" as follows (see List of Items Controlled). "Software" for computerized finger-print equipment controlled under ECCN 4A003 for CC reasons is controlled under ECCN 4D001 for CC reasons.

d.) 4D980: "Software" "specially designed" for the "development," "production" or "use" of commodities controlled by 4A980.

e.) 4E001: "Technology" as follows (see List of Items Controlled).

Under this entry, “software” for computerized finger-print equipment controlled under ECCN 4A003 for CC reasons is controlled for CC reasons.

f.) 4E980: “Technology” for the “development,” “production” or “use” of commodities controlled by 4A980.

g.) 6A002: Optical sensors and equipment, and “components” therefor, as follows (see List of Items Controlled). The relevant control statement reads as follows: “CC applies to police-model infrared viewers in 6A002.c.”

h.) 6E001: “Technology” according to the General Technology Note for the “development” of equipment, materials or “software” controlled by 6A (except 6A991, 6A992, 6A994, 6A995, 6A996, 6A997, 6A998, or 6A999.c), 6B (except 6B995), 6C (except 6C992 or 6C994), or 6D (except 6D991, 6D992, or 6D993).

Within this entry, “technology” for equipment controlled under ECCN 6A002 for CC reasons (i.e., 6A002.c) is also controlled for CC reasons. Therefore, this entry subparagraph controls development technology for both 'direct view' imaging equipment with certain features and the related software.

i.) 6E002: “Technology” according to the General Technology Note for the “production” of equipment or materials controlled by 6A (except 6A991, 6A992, 6A994, 6A995, 6A996, 6A997, 6A998 or 6A999.c), 6B (except 6B995) or 6C (except 6C992 or 6C994).
CC applies to “technology” for equipment controlled by 6A002 for CC reasons (i.e., 6A002.c). Therefore, this controls *production technology* for ‘direct view’ imaging equipment with certain features and development *technology* for ‘Direct view’ imaging equipment with certain features and the related software.

Submission of Comments

All comments must be submitted to one of the addresses indicated in this notice. The Department requires that all comments be submitted in written form. BIS will consider all comments received on or before **[INSERT 60 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. All comments, including those comments containing any personally identifying information or information for which a claim of confidentiality is asserted in the comments or their transmittal emails, will be made available for public inspection and copying. Parties who wish to comment anonymously may do so by submitting their comments via Regulations.gov, leaving the fields that would identify the commenter blank and including no identifying information in the comment itself.

Richard E. Ashooh,

Assistant Secretary for Export Administration.

[FR Doc. 2020-15416 Filed: 7/16/2020 8:45 am; Publication Date: 7/17/2020]