Department of Homeland Security
DHS Directives System
Directive Number: 026-11
Revision Number: 00
Issue Date: 9/11/2023
Certified Current Date: 9/11/2023

USE OF FACE RECOGNITION AND FACE CAPTURE TECHNOLOGIES

I. Purpose

This Directive establishes an enterprise policy for the authorized use of Face Recognition (FR) and Face Capture (FC) technologies by the Department of Homeland Security (DHS). For the purposes of this Directive, FR technology compares an individual's facial features to available images or video for verification or identification purposes. Verification is the process of confirming an identity claim through FR comparison. Identification is the process of searching against an FR enrollment database to find and return the FR reference identifiers attributable to a single individual or multiple possible candidates. FC technology is defined as any combination of face detection and face collection technologies used to detect and/or extract a face from an image or video, and for the purposes of this Directive, includes liveness detection used to detect the presence of a live user. Face Analysis (FA) technology, for the purposes of this Directive, is defined as the use of an algorithm to estimate characteristics of a subject by analyzing or deriving information from an image or video.

II. Scope

This Directive applies to the use of FR and FC technologies for any purpose and limits the use of FA technology, including technologies used by Federal, State, Local, Tribal and Territorial government, non-U.S. government, and international entities operated by or on behalf of the Department. This Directive does not apply to the research, development, test, and evaluation of FR or FC technologies that are both (1) conducted under the oversight of the Under Secretary for Science and Technology (USST) and (2) are not used in DHS operations to inform processes or decision making. This Directive does not supersede DHS privacy and civil rights and civil liberties regulations and policies. This Directive does not apply to the DHS Office of Inspector General.

III. Authorities

A. The Immigration and Nationality Act, as amended, §§ 215 (8 U.S.C. § 1185), and 235 (8 U.S.C. § 1225).

B. The Illegal Immigration Reform and Immigrant Responsibility Act of 1996, as amended, Public Law 104-208 (8 U.S.C. § 1365a).

C. The Intelligence Reform and Terrorism Prevention Act 0f 2004, as amended, Public Law 108-458 (8 U.S.C. § 1365b and 6 U.S.C. § 112).

D. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, as amended (8 U.S.C. § 1379).

E. The Enhanced Border Security and Visa Entry Reform Act of 2002, as amended, Public Law 107-173 (8 U.S.C. §§ 1721, 1722, and 1731).

F. The Homeland Security Act of 2002, as amended, Public Law 107-296, § 101 (6 U.S.C. § 111), 222, (6 U.S.C. § 142), 402 (6 U.S.C. § 202), 411 (6 U.S.C. § 211), and 892 (6 U.S.C. § 482).

G. The Federal Information Technology Acquisition Reform Act (FITARA), Public Law 113-291 (40 U.S.C. § 11319)."

H. The Federal Information Security Modernization Act (FISMA), 44 U.S.C. §§ 3551 - 3558.

I. Executive Order (E.O.) 13960, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," December 3, 2020.

J. E.O. 14074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety," May 25, 2022.

K. DHS Delegation 04000, "Delegation to the Chief Information Officer"

IV. Responsibilities

A. ***Under Secretary for Management***, through the DHS Chief Information Officer, is responsible for all aspects of this Directive.

B. ***DHS Chief Information Officer (CIO)*** is responsible for overseeing FR and FC technologies and related infrastructure in support of DHS missions and activities.

1. Oversees the acquisition, management, and implementation of FR and FC technologies per applicable regulations and policies for use in support of mission requirements.

2. Approves all FR and FC technologies for Component use in coordination with the impacted Component Head(s) and in accordance with the Directive, relevant law, DHS policy, and implementation instructions.

3. Consults and collaborates with the Under Secretary for Strategy, Policy, and Plans to ensure FR and FC technologies are only used in accordance with the Department's policy objectives.

4. Tracks all uses of FR and FC technologies for the Department.

5. Authorizes DHS representation to committees, subcommittees, and ad hoc working groups that develop and execute policies, programs, procedures, and technical criteria pertaining to the use of FR and FC technologies.

C. ***Under Secretary for Science and Technology*** is responsible for the Department's scientific, engineering, and analytical support of FR and FC technologies and ensures compliance with Department-wide strategies and policies within Science and Technology (S&T) authorities. S&T, in consultation and coordination with Component Heads and DHS Headquarters (HQ) Offices:

1. Develops accuracy and performance metrics, and procedures for testing and evaluating FR and FC technologies in accordance with International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) standards and technical guidance issued by National Institute of Standards and Technology (NIST).

2. Provides guidance, technical expertise, and oversight for testing and evaluating FR and FC technologies per ISO/IEC standards and/or technical guidance issued by NIST prior to operational use and as needed thereafter. Provides recommendations to Components on independent third-party testing and evaluation services approved by S&T.

3. Ensures compliance with applicable laws, regulations, and policies for the protection of human research subjects per the USST's role and authority as the DHS Human Subjects Protection Official (HSPO).

4. Submits results of testing and evaluation to the Component Heads and the DHS CIO, the Chief Privacy Officer, and the Office for Civil Rights and Civil Liberties within 30-days of completion of evaluation or with the FR and FC technology approval packages as applicable. Provides performance metrics data and analysis support, including technical assistance, in the evaluation and analysis of pre- and post-deployment performance metrics.

5. Reviews and updates FR and FC technology performance metrics and test and evaluation methodologies periodically, to ensure compliance with the latest applicable ISO/IEC standards and NIST guidance.

D. ***Under Secretary for Strategy, Policy, and Plans*** leads the development

of and ensures compliance with Department-wide strategies and policies regarding the use of FR and FC technologies.

1. Establishes DHS policy, provides guidance, and develops strategies for the development, acquisition, and implementation of FR and FC technologies that are operationally required and technically feasible.

2. Consults and collaborates with the DHS CIO and Component Heads to ensure FR and FC technologies are only authorized for use in accordance with this Directive, relevant law, and DHS policy.

E. ***Chief Privacy Officer*** has primary responsibility for both DHS privacy and information disclosure policy and exercises statutory oversight to ensure the use of FR and FC technology by DHS sustains, and does not erode, privacy protections for the collection, use, retention, dissemination, or disclosure of personally identifiable information (PII).

1. Reviews and approves Privacy Compliance Documentation for DHS use of FR and FC technologies, as applicable.

2. Performs periodic Privacy Compliance Reviews of DHS use of FR and FC technologies to verify compliance with DHS privacy policy.

F. ***Office for Civil Rights and Civil Liberties*** exercises statutory oversight of the impact of the use of FR and FC technologies by DHS to ensure they do not diminish the civil rights and civil liberties of persons. This includes, but is not limited to, minimizing bias in operational use, and safeguarding individuals against disparate impacts based on protected characteristics.

G. ***General Counsel*** provides legal review, guidance, and advice to ensure that appropriate authorities exist for the use of FR and FC technologies by or on behalf of DHS in coordination with Component counsel, as appropriate.

H. ***DHS Chief Information Security Officer*** ensures all FR and FC technologies used by or on behalf of DHS are compliant with DHS Sensitive Systems Policy 4300A and DHS National Security Systems Policy 4300B, as applicable. Publishes and maintains security standards and risk management instructions for FR and FC technologies used by or on behalf of DHS.

I. ***Component Head*** is the senior official responsible for the implementation and use of FR and FC technologies within their Component or Office:

1. Approves the Components operational use of FR and FC technologies in coordination with the CIO and in accordance with the Directive, relevant law, DHS policy, and implementation instructions.

2. Ensures that FR and FC technologies are only used by their Component or Office in support of authorized DHS missions and approved per this Directive, implementation instructions, relevant law, and DHS policy.

3. Ensures that staff operating FR and FC technology programs are trained in its use in accordance with the requirements of this Directive.

V. Policy and Requirements

A. Policy

1. It is incumbent upon DHS to ensure that regulations, policies, and governance exist to provide effective oversight of FR and FC technologies across the Department and for mission partners. FR and FC technologies are critical capabilities that enable DHS to execute its mission to protect the American people from threats to their security. These technologies continue to transform how the Department delivers its services, including improving the customer experience, supporting DHS's law and civil enforcement missions, and securing our borders. The potential of this technology is expansive with new applications emerging frequently.

2. FR and FC technologies at DHS are only authorized for use for DHS missions, in accordance with DHS' lawful authorities, applicable statutes, regulations, and DHS policies. Further, DHS continues to anticipate and assess the impacts and operational risks of FR and FC technologies across the Department with strong leadership oversight and ongoing testing and evaluation of the technologies.

3. FR and FC technologies are inherently privacy sensitive. Therefore, it is essential that DHS only uses FR and FC technologies in a manner that includes safeguards for privacy, civil rights, and civil liberties. DHS continually strives to minimize bias and disparate impact on protected groups and does not collect, use, disseminate, or retain FR or FC information solely based on race, ethnicity, national origin, religion, gender, gender identity, age, sexual orientation, medical condition, or disability. DHS does not use FR or FC technologies to profile, target, or discriminate against any individual solely for exercising their Constitutional rights or to enable systemic, indiscriminate, or wide-scale monitoring, surveillance, or tracking.

4. DHS Components ensure that FR and FC technologies are independently tested and evaluated under the oversight of S&T to meet applicable performance metrics, ISO/IEC standards, and NIST guidelines prior to operational use, and at least every three (3) years during

operational use. Results from testing and evaluation of FR and FC technologies performed by third parties may be accepted when less than three (3) years old and upon evaluation and approval by S&T.

5. When FR technology is used for verification for non-law enforcement related actions or investigations:

a. DHS affords U.S. citizens the right to opt-out and ensures alternative processing is available, unless otherwise authorized or required by statute or regulation. FR technology for verification may not be the sole basis for denial for an administrative determination.

b. DHS ensures alternative processing is available to resolve match or no match outcomes. The mechanism or process to opt-out and complete alternative processing may not impose additional burdens or requirements on the individual beyond what is necessary to complete the verification process.

6. FR technologies used for identification may not be used as the sole basis for law or civil enforcement related actions, especially when used as investigative leads. Any potential matches or results from the use of FR technology for identification are manually reviewed by human face examiners prior to any law or civil enforcement action.

7. Sharing of FR and FC information collected, used, or maintained by DHS is limited in accordance with applicable authorities, statutes, regulations, information sharing and access agreements (ISAA), and policies. FR or FC information generated or shared by DHS outside the Department or with international entities may not be repackaged, re-shared, or sold by said entities.

8. All FR and FC technologies are secured against cybersecurity threats and risks in compliance with the DHS Information Technology Security Program.

9. If within DHS's or a Component's mission, exigent circumstances require an FR or FC technology for a new use, the respective Component Head requests an expedited provisional 30-day approval in writing by the DHS CIO with notice to the Under Secretary for Strategy, Policy, and Plans, the Chief Privacy Officer and the Office for Civil Rights and Civil Liberties. Any use of FR or FC technology provisionally approved by the DHS CIO under exigent circumstances complies with the requirements of this Directive and accompanying Instruction and initiates compliance actions within 30-days of provisional approval. Should the provisional approval expire prior to the expiration of the exigency, the Component Head may request one additional provisional 30-day approval from the

DHS CIO in coordination with the Under Secretary for Strategy, Policy, and Plans, the Chief Privacy Officer and the Office for Civil Rights and Civil Liberties.

10. FA technology is not authorized for use at DHS except for specific uses related to estimating age which may be authorized for use when in compliance with this Directive and the Instruction and when specifically approved by the Chief Privacy Officer, the Office for Civil Rights and Civil Liberties, the Under Secretary for Strategy, Policy, and Plans, and the DHS CIO.

B. ***Requirements***

FR and FC technologies are a critical enabler of DHS capabilities to execute its diverse and critical mission. Use of the technology is driven by current and projected homeland security requirements and implemented by the Department in a manner to provide the greatest overall benefit to DHS missions while safeguarding privacy, civil rights, and civil liberties. Additional Instructions or any associated manuals and guides that fall within this Directive's scope are controlled and managed by a process established through this Directive's implementing Instructions and managed by the DHS CIO in coordination with Under Secretary for Strategy, Policy, and Plans.

VI. Questions

Address any questions or concerns regarding this Directive to the DHS Chief Information Officer.

RANDOLPH D ALLES

Digitally signed by RANDOLPH D ALLES
Date: 2023.09.11 11:02:09 -04'00'

R.D. Alles
Deputy Under Secretary for Management

Date