OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN FOCUS

4 MARCH 2021 IA-49515-21

BORDER SECURITY

(U//FOUO) European Union: Legacy Border Security Challenges Present DHS Engagement Opportunities

(U//SBU) ***The European Union (EU) continues to bolster border security and aspects of its migration enforcement, although it will likely continue to struggle to find equitable resettlement solutions or manage the movement of migrants.*** EU member states have long struggled to find consensus on migration policy, with Mediterranean countries shouldering much of the responsibility of continued migrant arrivals, some of whom have gone on to conduct terrorist attacks. A spate of terrorist attacks in the EU during the fall of 2020 prompted calls by member states to strengthen border security and counterterrorism (CT) measures, according to US government information reporting and Western press.

- *(U)* Following terrorist attacks in France and Austria late last year, the EU launched new efforts to strengthen CT and border security capabilities, including resolutions to improve law enforcement collaboration and information sharing among member states and strengthen the European Union Agency for Law Enforcement (EUROPOL) mandate to improve data processing and allow further cooperation with the private sector and non-EU countries, according to the EU and Western press. Additionally, the EU approved billions of euros to support further integration of external border management, including interoperability between major law enforcement and border security information systems, and harmonize protocols for long term visa issuance according to EU information.

- *(U//SBU)* In September 2020, the EU proposed a new common migration policy which calls for more cooperation with non-EU countries to stop migrant departures, increased repatriations, and more shared responsibility among member states to re-settle migrants. However, the new pact is opposed by several Central European governments and new compromises allow member states to opt-out of receiving refugees in exchange for providing financial and administrative assistance, increasing the likelihood that the primary responsibility for receiving and hosting migrants will remain with border states such as Spain, Italy, Greece, and Malta, according to US government information, a US think tank, and Western press.

- *(U)* In 2019, the EU bolstered the operational support capabilities of the European Border and Coast Guard Agency, also known as Frontex, and agreed to create a standing corps of 10,000 border and coast guards—changes that are still being implemented, according to the EU and FRONTEX as well as Western press. Additionally, in 2018, Frontex launched new joint operations in the Central Mediterranean Sea to secure EU borders,

(U) Prepared by the Counterterrorism Mission Center. Coordinated within the DHS Intelligence Enterprise (CBP, CWMD, ICE, USCIS).
For questions, contact DHS-SPS-RFI@hq.dhs.gov

with an enhanced focus on law enforcement, including the detection of terrorist travelers at external borders.

- *(U//SBU)* Since 2016, many Schengen countries have maintained some level of internal border checks to curb illicit travel, although the EU still has only limited ability to monitor internal migrant travel.[a] In October 2020, a Tunisian migrant who was released shortly after arriving in Italy due to lack of known criminal or terrorist connections, immediately traveled undetected to Nice, France, and conducted a stabbing attack, according to US government information and Western press. As of October, over 11,000 Tunisians had traveled to Italy in 2020, but only 80 persons are repatriated weekly to Tunisia, leaving large numbers of migrants able to travel further into Europe with minimal scrutiny, according to US government information.

(U//SBU) ***Renewed focus on strengthening external border security likely provides additional opportunities for DHS engagement with the EU and individual member states.*** Standing and deployable DHS screening platforms, along with DHS expertise in creating and consolidating new screening mechanisms would likely complement ongoing EU efforts to modernize and expand traveler and migrant screening. However, challenges to deeper engagement remain in part due to technical impediments and delays in program implementation, according to DHS and EU information.

- *(U)* The EU's Smart Borders package consists of two screening platforms—one of which is modeled after CBP's Electronic System for Travel Authorization—which will register and prescreen all third-country nationals entering the Schengen Area against European law enforcement and registration systems as well as a dedicated watchlist, according to EU information. The other platform, the Entry/Exit System, registers travelers entering the EU every time they cross an external EU border, linking their name, biometric data, and date and place of entry or exit, resulting in more secure travel, according to EU information.

- *(U//FOUO)* Implementation of DHS's Secure Real Time Platform (SRTP) with Mediterranean states, notably Greece, Italy, and Spain, has had mixed results. Greece incorporated SRTP into its screening systems in 2016 and is the only EU country to fully implement the program following years of technical and operational delays, according to DHS information. DHS began SRTP implementation discussions with Italy in 2018, but progress has been slow due largely to Rome's resistance to establish required technical connections, while engagement with Spain has been sporadic and has yet to gain sufficient traction due to Madrid's focus on domestic politics, according to DHS information.

- *(U//FOUO)* DHS has deployed BITMAP, the Biometric Identification Transnational Migration Alert Program, in Bosnia-Herzegovina, Bulgaria, and Malta and continues to look for new partners. BITMAP implementation in Europe relies on an identified need, a

[a] *(U)* The Schengen Area comprises 26 European countries that have abolished internal border controls to allow for the free and unrestricted movement of people. Most Schengen countries, although not all, are also EU member states. Member countries include Italy, France, Germany, and Spain.

demand signal, a willing host country partner, and approval from the US Department of State, while funding sources and availability of personnel are the only major obstacles for implementation, according to DHS information.

(U//FOUO) **Key Screening and Information Sharing Arrangements**

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

	SRTP	BITMAP	IAP	ATS-G	GTAS
Bosnia-Herzegovina		✓			
Bulgaria	*Pending*	✓			
France			✓		
Greece	✓			✓	
Italy	*Pending*				
Malta		✓			
Spain			✓		

(U) **Highlights of the EU's Upcoming Smart Borders Package**

(U) **The European Travel Information and Authorization System (ETIAS):** ETIAS will be operated by Frontex and will conduct pre-travel screening of all visa-exempt travelers against European and law enforcement databases such as SIS, VIS, INTERPOL and EURODAC, in order to identify potential security concerns, according to EU information. ETIAS will be operational by the end of 2022 and its watchlist will be maintained by its central unit with input from INTERPOL and EU member states, according to the same source.

(U) **The Entry/Exit System (EES):** EES will be implemented in the first half of 2022 and will register border crossings of both visa-exempt and visa-required travelers, including US citizens, into the Schengen Area. EES confirms a traveler's identity by linking travel documents to a single biometric record and screens all travelers against EUROPOL and EU member state law enforcement databases, according to EU information.

(U) **Interoperability**: the EU passed legislation in 2019 to strengthen its identity management databases and ensure interoperability with existing and new screening systems, such as the Smart Borders package. This includes establishing a Common Identity Repository and a centralized biometric matching system to connect previously stand-alone information systems like the Schengen Information System, the Visa Information System, and EURODAC, according to EU information and Western press. This information will be shared with EUROPOL to prevent terrorist or criminal offenses.

Source, Reference, and Dissemination Information

Source Summary Statement	(U) We have **high confidence** in our assessment that the European Union will continue to face counterterrorism challenges despite its efforts to reform and bolster external border security of the Schengen zone based on US government information, European Commission, and Western press reporting. We have **high confidence** in our assessment that our European partners will seek DHS engagement as such enhanced engagement will be mandatory for members of the Visa Waiver Program, and also may dovetail with implementation of the Smart Borders Package next year, based on US government requirements, government-to-government exchanges, and US government information.
Reporting Suspicious Activity	(U) **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx. (U) **To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us- cert.gov/report/ and complete the US-CERT Incident Reporting System form.** The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.
Dissemination	(U) Policymakers across the Department of Homeland Security as well as the broader US Government.
Warning Notices & Handling Caveats	(U) **LAW ENFORCEMENT SENSITIVE:** The information marked (U//LES) in this document is the property of DHS and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials, and individuals with a need to know. Distribution beyond these entities without DHS authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network. (U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may not share this document with critical infrastructure and key resource personnel or private sector security officials without further approval from DHS.

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) European Union: Legacy Border Security Challenges Present DHS Engagement Opportunities

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

□ Drive planning and preparedness efforts, training, and/or emergency response operations
□ Observe, identify, and/or disrupt threats
□ Share with partners
□ Allocate resources (e.g. equipment and personnel)
□ Reprioritize organizational focus
□ Author or adjust policies and guidelines
□ Initiate a law enforcement investigation
□ Intiate your own regional-specific analysis
□ Intiate your own topic-specific analysis
□ Develop long-term homeland security strategies
□ Do not plan to use
□ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:
Position:
State:
Email:

Submit Feedback

Privacy Act Statement

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Product Serial Number: IA-49515-21