New York Memorandum on Good Practices for Interdicting Terrorist Travel

Introduction

As foreign terrorist fighters (FTFs) are pushed from territory once held by ISIL/Da'esh, states should take proactive measures to ensure those travelers are detected, identified, tracked, and where appropriate, interdicted. The effective implementation of enhanced terrorist screening mechanisms and international cooperation for information sharing are key to that effort.

In December 2017, the United Nations Security Council adopted UN Security Council Resolution (UNSCR) 2396. This resolution requires Member States to develop and implement systems to collect biometric data and to develop watchlists or databases of known and suspected terrorists (KSTs), including FTFs. Member States are also obligated to collect and analyze Advance Passenger Information (API) and Passenger Name Record (PNR) data in border screening to deter the travel of known and suspected terrorists, and to require airlines operating in their territories to provide API to the appropriate national authorities. Analysis of PNR can help a country identify previously unknown links between terrorists and other travelers. Additionally, UNSCR 2396 encourages Member States to share this information through bilateral and multilateral mechanisms. Implementing these UNSCR provisions can be complex, resource-intensive, and expensive.

In recognition of these challenges, in September 2018, Morocco and the United States launched an Initiative under the auspices of the Global Counterterrorism Forum (GCTF) Foreign Terrorist Fighters Working Group to provide guidelines for improving terrorist screening mechanisms and capabilities to interdict terrorist travel. This document is the result of lessons learned, concerns, challenges, and case studies shared by practitioners and policymakers to address systemic gaps and implement necessary legal and policy measures to further secure borders against terrorist travel and ensure implementation of UNSCR 2396.

Moreover, this document synthesizes the major themes and outcomes from regional workshops in New York, the United States; Berlin, Germany; Kuala Lumpur, Malaysia; and Rabat, Morocco. The following non-binding guidelines for good practices should be considered in light of each state's circumstances, domestic legal standards, and international obligations and commitments, including those under international human rights law, international refugee law, and international humanitarian law, as applicable.

Good Practices

I. Legal and Policy Frameworks

Good Practice 1: Establish legal and policy frameworks for watchlisting to facilitate the creation of a national-level watchlist and a comprehensive watchlisting and screening process.

Legislation and policy directives may be necessary to allow a nation's security agencies to create a cohesive and streamlined watchlisting process that is consistent with international law obligations. Organizing whole-of-government watchlisting policy and guidelines can ensure maximum efficiency and effectiveness for detecting and interdicting terrorist travel. Legislation should include a basis to compel passenger carriers to provide passenger data, including Advance Passenger Information and/or Passenger Name Records (API/PNR), to appropriate authorities via a single window and specified systems.

Authorities should also incorporate measures to safeguard the integrity of the screening process and privacy of personal information, particularly pertaining to the collection and utilization of biometrics and API/PNR data. The operation of watchlists should be subject to independent and transparent oversight, such as judicial scrutiny. An independent delisting mechanism will help to safeguard human rights and ensure fair trial guarantees, and states might consider whether the courts should have a role in placing identities on a watchlist or removing them to safeguard the same (see Good Practices 4 and 16). Legal and policy frameworks should include guidelines specifying the identity information included in screening systems, permissible reasons for the use of identity information, how long such identity information will be retained, standards for data integrity and protection, and procedures to challenge and rectify unlawful, inappropriate, or mistaken inclusion on a watchlist (see Good Practice 16). Within the framework, clearly defined authority should be established to release certain biographic and biometric identifiers appropriately for watchlisting and screening purposes only.

Organizing and outlining national interagency watchlisting processes and procedures in a document, based on legal and policy guidelines, will help ensure uniform use of watchlisting across government and will institutionalize watchlisting and screening processes for identifying and interdicting terrorist travel (see Good Practice 5). When developing national interagency watchlisting processes and procedures, all stakeholders (originators, nominators, watchlisters, and screeners) should discuss potential new procedures to consider the full effects. [1]

[1] This document uses the following definitions: **Originator** refers to the entity that initially collects and identifies information supporting the conclusion that a person is a known or suspected terrorist. **Nominator** is the entity that has information to indicate that a person meets the criteria for a known or suspected terrorist and nominates that person to a watchlist based on information that originated with that entity. **Watchlister** is the entity that maintains the watchlist of known or suspected terrorists, including accepting nominations and providing relevant information to screeners. **Screener** is the entity that uses watchlist information to determine if a person is a possible match to a known or suspected terrorist.

Good Practice 2: Organize and apply international standards for watchlisting processes, and base API/PNR legislation on current international standards and practices.

International organizations such as the World Customs Organization (WCO), the International Civil Aviation Organization (ICAO), and the International Air Transport Association (IATA) have developed standards and recommended practices to support passenger data screening that states should consider incorporating. ICAO has promulgated standards and recommended practices on API, and is currently developing them for PNR, in annexes to the ICAO *Convention on International Civil Aviation* (Chicago Convention), which will provide an established international legal framework to promote cooperation in civil aviation security, border integrity and facilitation; and, is an effective tool to streamline capabilities.[2] Annex 9 on the Facilitation to the Chicago Convention contains Standards and Recommended Practices (SARPs) for API and PNR. These provisions reference the guidance material and API/PNR message implementation guidelines developed by the WCO, IATA and ICAO. All states should follow the international regulatory framework when implementing API/PNR programs. The GCTF *Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of 'Foreign Terrorist Fighters'* have also outlined good practices on border security and international cooperation that can further serve as a roadmap for states.[3] Moreover, the *Abuja Recommendations on the Collection, Use, and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects* and related GCTF Good Practice Documents provide guidance on data handling and case management for terrorism-related legal proceedings.[4] The UN has issued a *Biometrics Compendium* to help guide states that are in the process of integrating biometric technologies into their systems to identify and interdict terrorist travel.[5]

States might consider collaborating to forge compatibility among standards for watchlist inclusion, data fidelity, information collection methods, and permissible uses of database information. This compatibility of basic watchlisting standards for inclusion could be codified through legislation or policy agreements, while noting potential limitations due to sovereign nation's laws. Interoperability can streamline the detection and interdiction of terrorist travel by increasing trust among international partners, reducing ambiguity over actions to take during interactions, enhancing compatibility between screening systems, and ensuring that watchlisting and information-sharing practices are consistent with the prohibition on arbitrary or unlawful interference with privacy and other human rights obligations and commitments.

---

[2] International Civil Aviation Organization, *Annex 9 to the Convention on Civil Aviation ("Chicago Convention"): Facilitation*, October 2017.

[3] GCTF, *Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of "Foreign Terrorist Fighters,"* Good Practice 3. www.theGCTF.org.

[4] GCTF, *Abuja Recommendations on the Collection, Use, and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects.* www.theGCTF.org.

[5] UNOCT, UNCTED, and Biometrics Institute, *United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-terrorism*, 2018.

Good Practice 3: Develop mechanisms, standards, and where necessary enact legislation to exchange information internationally.

The importance of sharing watchlist information about KSTs in a sustained, systematic, and complete – rather than ad hoc, intermittent, and incomplete – manner that respects human rights cannot be overstated. Sharing should occur based on mutual agreement and include sufficient unclassified biographic and contextual information to inform any actions that the information-sharing states may take in the event of an encounter (see Good Practice 9). Such sharing should occur independent and regardless of travel, enabling analysis prior to travel and timely receipt of relevant information.[6] States should consider signing written arrangements to define the terms of information sharing relationships and to include required protection and permitted use of exchanged information.

Data and privacy protection legislation should include sufficient allowances for passenger carriers to disclose appropriate passenger and crew data to a foreign country for the purposes of countering terrorist travel, provided proper privacy protections and legal basis exist (see Good Practice 14).

Good Practice 4: Establish independent oversight mechanisms to ensure standards for database inclusion.

Appropriate oversight not only helps ensure the protection of human rights and fundamental freedoms but also enhances national security. Safeguarding a watchlist database from inclusion of insufficient or unlawful data or from politically motivated inclusion of identities with no nexus to terrorism, and ensuring watchlisting and screening processes meet agreed upon standards, helps assure both watchlist users and the public of the quality, integrity, and value of the watchlist. An independent monitoring authority can ensure legal and data integrity requirements are met. An oversight organization can produce a periodic report to ensure watchlisting and screening activities are conducted in accordance with applicable domestic law and directives, interagency processes and procedures, and international obligations. Such an organization may recommend corrective actions to remedy deficiencies and propose procedures to align domestic practices with applicable international law and good practices.[7]

---

[6] GCTF, *The Hague–Marrakech Memorandum on Good Practices for a More Effective Response to the FTF Phenomenon,* Good Practices 10 and 12. www.theGCTF.org.

[7] The UN's *2018 Addendum to the 2015 Madrid Guiding Principles* provides further guidance on developing watchlists and working alongside bilateral and multilateral partners.

II. Development and Implementation of Screening Systems

Good Practice 5: Engage the whole-of-government in the development and implementation of screening systems.

To ensure the thorough, accurate, and timely processing of information in screening systems, states should ensure interoperability between and within government agencies.[8] This includes developing definitions and articulable legal standards for watchlist inclusion, and harmonizing data formats and system requirements. States might consider enacting legislation to achieve this. Ensuring internal government systems are interoperable allows timely access to watchlist-relevant data across agencies and systems, and helps ensure consistent implementation of legal and policy frameworks.[9] When in the early stages of developing watchlist systems, states should also ensure that operational staff and IT staff are collaborating so the watchlist meets the needs of the operators and is technically feasible. Input from all watchlist users should be accounted for prior to system development. Ensuring government agencies share information among each other as a matter of practice is important to facilitating appropriate responses to interactions with individuals on a watchlist. Information to be shared could include battlefield evidence and biometrics collected or processed by military personnel (see also Good Practices 10 and 12).

Relevant government agencies should work together to create and organize watchlisting and screening processes and procedures that act upon and implement higher-level legal and policy directives and guidelines. The resulting document should institutionalize agency roles and responsibilities in providing information to, and using information on, a watchlist. The document should establish watchlisting definitions, standards, and general data requirements such as biographic and biometric requirements as well as data retention practices. The document should be updated routinely and made available for all watchlist users, to include policy, legal, and operational stakeholders (see Good Practice 1).

States might consider designating a single agency to become the clearinghouse for passenger information to process data and flag watchlisted passengers to appropriate authorities. Such a "single window" can help to minimize bureaucratic delays, reduce costs, and prevent inappropriate access to database information.

Good Practice 6: Engage international partners in the development and implementation of screening systems.

States might consider partnering with other states or with international organizations that have specialized experience with screening systems and that offer support and IT tools to ensure

---

[8] GCTF, *The Hague–Marrakech Memorandum on Good Practices fora More Effective Response to the FTF Phenomenon,* Good Practice 11. www.theGCTF.org.

[9] GCTF, *Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of "Foreign Terrorist Fighters,"* Good Practice 2. www.theGCTF.org.

effectiveness and long-term sustainability of such systems.[10] Several states offer support to other countries by sharing their own legislation and implementation guides, providing training, and offering technical support. International organizations, such as the UN Office of Counter-Terrorism[11], the WCO, and Organization for Security and Co-operation in Europe (OSCE) offer capacity building programs and software solutions for enhancing terrorist screening capabilities.

Good Practice 7: Engage relevant air carriers and industry partners to streamline the development and implementation of screening systems.

Where possible and appropriate, consult, partner, and cooperate with relevant industry stakeholders, to include domestic and multinational carriers, in the establishment of regulatory foundations and technical specifications of screening systems. This engagement can secure buy-in from private industry partners charged with implementing passenger data transfer regulations where they exist, and can ensure compliance and efficient data transfer. Private industry stakeholders may have experience implementing such systems elsewhere and can offer procedural expertise for implementation to align with international good practice and ensure compatibility of national systems. States might consider partnering with a single air carrier initially to beta-test functionality, which can serve as a trial for industry-wide implementation. Preparing a technical implementation document for private industry that includes the information required for transmission, the standards for transmission, and a timeline for compliance can help to ensure effective design and operation of screening systems.

Good Practice 8: Assess available resources, capabilities, and needs for the development of screening systems.

States have options when considering implementation of passenger screening systems, and states should choose systems that align with their needs and capacity. The use of API and PNR in border screening should enhance and ultimately improve traveler facilitation by allowing border officials to focus their attention on passengers of highest risk. Indigenously developed systems for processing and cross-referencing API/PNR data may minimize initial costs but often require greater capacity for maintenance and reliance on expensive, highly skilled staff. Alternatively, states have the option of working with commercial, multilateral, or bilateral partners in the development and implementation of such systems (see Good Practice 2). States also should implement strategies that align with international standards to ensure compatibility with existing airline systems, take advantage of efficiencies, reduce costs, and accelerate implementation. In

[10] OSCE, *Outcome Document from the 2nd OSCE-wide Seminar on Passenger Data Exchange*," SEC.GAL/190/18 (3 December 2018). www.osce.org.

[11] UNOCT coordinates a capacity building effort based on the goTravel software system, which is offered to Member States in the process of developing and implementing passenger data transfer systems with technical and technological assistance free of charge. https://www.un.org/cttravel/goTravel.

support of the international legal framework contained in ICAO Annex 9, the WCO, ICAO, and IATA offer guidelines for states to implement such systems.[12]

Good Practice 9: Ensure screening systems offer timely access to current, comprehensive, and actionable data.

Authorities need access to current, specific, and accurate data to take appropriate and informed action. Systems should allow for reliable open source information, such as news or investigative reports found online, to quickly update information concerning watchlisted identities. The system should be flexible and allow for ingesting and exporting multiple data formats and future enhancements to datasets. The watchlist system should be supported by technicians via a help desk on a 24-7 basis so technical problems do not inhibit timely access to data. States should carefully consider the information fields required in their database. Enriching data with contextual information may empower authorities to take appropriate and timely action. Providing connectivity and routine updates of information from a watchlist to end-users is vital for providing comprehensive border security. All systems involved in traveler screening should have real-time connectivity and access to the national watchlist. Additionally, responsible government authorities should have access to the International Criminal Police Organization (INTERPOL) databases and relevant notices via the I-24/7 platform (see Good Practice 13). Analyzing passenger data as a process, through an automated targeting system – before, during, and after air, maritime, rail, and bus travel – can highlight patterns and provide more fidelity than assessments conducted in a vacuum.

Good Practice 10: Responsible collection and use of biometric information can add fidelity and accuracy to a screening database.

Biometric collection systems that are interoperable with screening and law enforcement systems can fuse information to more accurately identify KSTs. Biometrics greatly reduce the potential for falsely identifying an individual based solely on biographical data and can help detect people traveling on false documents by linking biometric data to passports. Any biometric data used as evidence in court should be collected legally, and collection of any evidence from the battlefield should be done in accordance with domestic and international obligations, as well as relevant good practices in the GCTF *Abuja Recommendations on the Collection, Use, and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects*.[13]

---

[12] ICAO, *Guidelines on Passenger Name Record (PNR) Data*, 2010; ICAO, *International Standards and Recommended Practices: Annex 9 to the Convention on International Civil Aviation "Chicago Convention" – Facilitation*, Chapter 9, October 2017; WCO, IATA, and ICAO, *Guidelines on Advance Passenger Information (API)*, 2014.

[13] GCTF, *Abuja Recommendations on the Collection, Use, and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorist Suspects,* Recommendations 20-21. www.theGCTF.org.

III. Information Sharing and Access

Good Practice 11: Cultivate a balance between "need to know" and "responsibility to share" by enhancing inter- and intra-agency cooperation.

For screening databases to function as intended, government agencies should break down resistance to sharing identity and underlying information among intelligence agencies and front-line authorities such as law enforcement, border screening, and consular officials. States might consider several strategies to encourage such cooperation while protecting sensitive intelligence information.[14]

Establishing a screening fusion center that collocates intelligence officers with law enforcement can be an efficient mechanism to ensure the timely integration of information into the appropriate database while providing access to the relevant authorities by offering near-real-time avenues for intelligence reach-back support. Alternatively, IT and technical solutions may serve the same purpose. Separating and protecting underlying classified information (intelligence or sourced information) in a separate database from unclassified identity and contextual information (the watchlist) protects intelligence channels and increases intelligence agencies' comfort with routinely sharing information for watchlisting purposes.

In cases where in-person reach-back may not be feasible, data-matching algorithms and computer analysis of searches or requests for information by front-line officials can unlock access to more sensitive screening information when warranted while protecting information integrity. Such tools are most useful when paired with interoperable systems that distribute and provide access to data across government agencies. Establishing a comprehensive information sharing cycle protects classified data while facilitating broad access to unclassified screening information, which allows for the enhancement of unclassified data with classified information when an encounter with an individual of interest warrants such access.

Good Practice 12: Organize watchlisting structures and processes to allow efficient and effective information access.

When organizing watchlist roles and responsibilities, watchlist administrators should be distinct from the agencies that originate, nominate, and screen against information to better ensure unbiased use and analysis of the quality and reliability of information. States should develop a standard to differentiate between high-risk and low-risk records, based on underlying derogatory threat information, to more easily manage information on a timely basis. Information access standards should be based on screening agencies' needs and capabilities, not on what is available in intelligence. Information derived from encounters with persons whose identity appears on a watchlist can be used to enhance records as appropriate. To increase efficiency in identifying

[14] See *2018 Addendum to the 2015 Madrid Guiding Principles,* Guiding Principle 2 for further guidance on integrating systems.

watchlisted individuals, multiple identities of one individual should be consolidated into a single entry, rather than listing an individual multiple times under various known identities.

Good Practice 13: Use existing multilateral databases to process passenger data and facilitate international exchange.

States should work with international law enforcement organizations such as INTERPOL to provide as much information as legally allowed on persons of concern and to screen travelers against all available information.[15] Providing consistent updates to INTERPOL will keep its databases accurate and relevant for all parties, and real-time screening against INTERPOL databases can be a force-multiplier. Equipping local law enforcement with access to INTERPOL databases can also help identify KSTs. States should provide all possible context to identities submitted to INTERPOL to assist police in making a decision on how to handle an encountered individual. States might also consider creating or enhancing regional databases for sharing screening information to identify and interdict region-specific terrorist travel.

IV. Privacy, Rights, and Redress

Good Practice 14: Take proactive measures to maintain the security and privacy of watchlist and passenger information.

States should ensure that data integrity measures are in place and standardized within international and national databases. The collection, storage, use, and sharing of passenger information and biometric data should continue pursuant to legally authorized means. Including a sunset clause in legislation or policy can be an effective way to ensure identities are removed from a watchlist when they no longer meet the inclusion standard (see Good Practices 1 and 5 on creating a strong national watchlisting guidance document).

In the absence of multilateral standards for watchlisting that protect data integrity and freedom from arbitrary or unlawful interference with privacy, the sensitive information underpinning a watchlist entry should be shared bilaterally through international arrangements that include data integrity and privacy measures.[16]

Good Practice 15: Align the collection and use of watchlist and passenger information with domestic laws and international obligations and commitments.

States should delineate clear and transparent risk-based standards to determine what identities, on the basis on reasonable and factual criteria, are appropriate to place on a watchlist. Identities

[15] GCTF, *Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of "Foreign Terrorist Fighters,"* Good Practice 3. www.theGCTF.org.

[16] OSCE, *Outcome Document from the 2nd OSCE-wide Seminar on Passenger Data Exchange*," SEC.GAL/190/18 (3 December 2018). www.osce.org.

should not be included on a watchlist for politically motivated purposes or any discriminatory grounds prohibited by international law. All information sharing arrangements should include safeguards to ensure that information provided by one partner to another is not misused for unauthorized purposes, such as to commit human rights violations or abuses. Controls should be in place, subject to appropriate review, to ensure watchlist and passenger information databases cannot be used for profiling on a basis that is inconsistent with states' obligations under applicable domestic law or international law.[17] In particular, states should ensure the use of watchlist and passenger information databases does not discriminate on the grounds prohibited by international law, such as race, color, sex, language, religion, political or other opinions, national or social origin, property, birth, or other status. Authorities with access to watchlist information should be appropriately trained on individuals' legal protections, including the human rights of each individual to enter their own country and to be equal before the law and receive equal protection by the law.[18]

Biometric information can be a powerful tool to enhance identification capabilities (see Good Practice 10), but it also presents a danger of revealing incidental and irrelevant personal private information that may be illegal or unethical to reveal without consent, or that may be used for illicit purposes. It is therefore necessary to ensure that biometric data is collected, stored, processed, and transmitted securely. Operating biometric systems in accordance with international standards and formal accreditation of forensic sciences can ensure the procedural safeguards and effective oversight to minimize that risk.[19]

Good Practice 16: Implement mechanisms to verify data entry accuracy, as well as for individuals to contest their status in a terrorist screening database ("redress").

Identities inadvertently or wrongly placed in a terrorist-screening database should have an accessible, clear, efficient, and appropriately transparent redress process to challenge, initiate a review, and remove any errant information. Challenges to suspected database inclusions should be subject to appropriate handling procedures to ensure classified or otherwise sensitive information is properly protected. Mechanisms for automated data review can identify errant information in an efficient and timely manner, and the ability for interagency stakeholders to request a review or redress of specific identities on the watchlist can be an effective way to maintain an accurate database, focus security resources on credible threats, and provide public confidence in national security programs.

---

[17] Article 12 of the *UN Universal Declaration of Human Rights* states clear parameters for the protection of individual privacy and protection of such rights under the law. https://www.un.org/en/universal-declaration-human-rights/.

[18] See: UNOCT, *Human Rights and Screening Border Security Pocketbook,* 2018 Edition. https://www.un.org/counterterrorism/ctitf/.

[19] For a deeper review of such biometrics tools and guidance see UNOCT, UNCTED, and Biometrics Institute, *United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-terrorism*, 2018, 52.

Conclusion

The full implementation of UNSCR 2396 is key to being able to detect and take appropriate measures to respond to terrorist travel. The exchange of experiences and good practices through this GCTF Initiative aims to facilitate the development and use of watchlists, biometric data, Advance Passenger Information, Passenger Name Records, and related tools for traveler screening to counter terrorist travel globally. This document is designed as a resource for states to develop and implement terrorist screening watchlist processes and systems as they comply with UNSCR 2396.

Fragmented or undeveloped interagency processes and limited screening or watchlisting capabilities may impede states' abilities to provide frontline screeners and law enforcement access to information critical to facilitating appropriate responses during interactions with KSTs. A comprehensive legal and policy framework is necessary for establishing a streamlined and appropriate screening process. States should develop a whole-of-government strategy to ensure watchlisting information is current, accurate, and actionable. Institutionalizing information sharing helps facilitate data exchange with relevant domestic stakeholders while protecting classified intelligence. Sharing information among national agencies is essential but should be complemented by appropriate international information exchange to counter global terrorist travel. Additionally, respecting privacy, human rights, and redress is important to ensure systems are not abused for political purposes and is essential for securing public acceptance of the data processing, watchlist management, and subsequent enforcement actions and protective operations.