UNISHKA
Research Service

Security Risk Analysis and Management Policy

September 2017

FOREWORD

This *Security Risk Analysis and Management Policy* is intended to mitigate the risk that UNISHKA Research Service (UNISHKA) will inadvertently provide support to entities or individuals deemed to be a risk to national security in contravention of established law.

All UNISHKA staff, consultants and affiliates are bound by this policy. Any deviation from these policies and procedures must be approved in writing by UNISHKA senior management.

UNISHKA welcomes your comments or suggestions for improvements and these may be incorporated in future revisions of these procedures.

Jeffrey Coonjohn 15 September 2017
CEO & Chief Operations Officer
UNISHKA Research Service, LLC

Contents

1 PURPOSE

The purpose of this *Security Risk Analysis and Management Policy* is to mitigate potential risk to UNISHKA; specifically, inadvertent support to entities or individuals deemed to be a risk to national security in contravention of established law.

2 OVERVIEW

International convention and United Nations (U.N.) resolutions, as well as United States (U.S.) statutes, regulations and executive orders prohibit UNISHKA from doing business of any kind with certain sanctioned individuals or entities. It is UNISHKA's responsibility to assess the risk of violation and mitigate that risk. This will require that UNISHKA regularly collect identifying information on persons or entities with whom it has financial or non-pecuniary relationships, and provide that identifying information to the appropriate party for screening (i.e. vetting). When project funds derive from funds appropriated to the U.S. Department of State (DoS) or the U.S. Department of Defense (DoD), UNISHKA must collect identifying information and submit it to the applicable agency for screening (e.g. DoD or DoS). When a project is privately funded, UNISHKA or the client must assess the risk of violation and, where appropriate, engage a Third Party Vendor to conduct the necessary screening.

3 RISK ANALYSIS & MANAGEMENT (RAM)

When a project is government funded, identifying information is customarily submitted to DoS for screening (i.e. vetting). The Risk Analysis and Management (RAM) System is a DoS effort to enhance review of organizations, entities, and individuals benefiting from U.S. government contracts, grants or other funding instruments. This program utilizes a centralized database to support the vetting process. Some of the databases the RAM screens against are:

- Consular Lookout and Support System
- Consular Consolidated Database
- Department of Homeland Security TECS
- Terrorist Identities Datamart Environment
- Terrorists Screening Database

When a project is privately funded, a commercial Third Party Vendor is the preferred method of screening. Companies such as eCustoms (i.e. Visual Compliance) can be contracted for privately funded projects to ensure compliance and risk mitigation.

4 SELECT LEGAL AUTHORITIES FOR VETTING

The legal basis for most vetting requirements derives from one or more of the following authorities. There are additional authorities, for example pertaining to the export of weapons, which are not applicable to UNISHKA and are, therefore, not listed.

4.1 Executive Order 13224:

In general terms, Executive Order 13224 provides a means by which to disrupt the financial support network for terrorists and terrorist organizations by authorizing the U.S. government to designate and block the assets of foreign individuals and entities that commit, or pose a significant risk of committing, acts of terrorism. In addition, because of the pervasiveness and expansiveness of the financial foundations of foreign terrorists, the Order authorizes the U.S. government to block the assets of individuals and entities that provide support, services, or assistance to, or otherwise associate with, terrorists and terrorist organizations designated under the Order, as well as their subsidiaries, front organizations, agents, and associates.

The Executive Order authorizes both the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, or the Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, to designate individuals and entities pursuant to specified criteria.

4.2 The Leahy Laws:

There are two "Leahy Laws," known as such due to Senator Leahy's authorship, one for DoS and DoD. The Leahy Laws apply to a "unit of the security forces." Individuals who are not members of the security forces but who participate in activities under an award – such as politicians, academics, community members, and so forth - generally do not need to be vetted under the Leahy Laws[1]. The U.S. government includes torture, extrajudicial killing, enforced disappearance, and rape under color of law as gross violation of human rights (GVHRs) when implementing the Leahy law.

[1] https://www.state.gov/j/tip/rls/other/2017/271082.htm

Incidents are examined on a fact-specific basis. "Security forces" may include any entity or unit – including individuals – authorized by a state or political subdivision – such as a city, county, commune, etc. – to use force to accomplish its mission. Security force and national defense force units in Bangladesh, Bolivia, Colombia, Guatemala, Mexico, Nigeria, Turkey, Indonesia, Lebanon, and Saint Lucia have been denied assistance due to the Leahy Laws.

4.3 Foreign Assistance Act of 1961, Sec. 620M

> *"No assistance shall be furnished…to any unit of the security forces of a foreign country if the [U.S.] Secretary of State has credible information that such unit has committed a gross violation of human rights."*

Beginning in 1998, Congress included in annual DoS appropriations acts language prohibiting assistance to any unit of the security forces of a foreign country if the Secretary of State has credible information that the unit has committed a GVHR. The DoS Leahy law is now codified as section 620M of Foreign Assistance Act of 1961.

The DoS Leahy law includes an exception permitting resumption of assistance to a unit if the Secretary of State finds and reports to Congress that the government of the country is taking effective steps to bring the responsible members of the security forces unit to justice.

4.4 10 U.S. Code §362

> *"None of the funds made available by this Act may be used to support any training program involving a unit of the security forces of a foreign country if the Secretary of Defense has received credible information from the Department of State that the unit has committed a gross violation of human rights, unless all necessary corrective steps have been taken."*

Since 1999, Congress has passed the DoD Leahy law in its annual appropriations act. The DoD Leahy law is now permanent in Section 362 of Title 10 of the U.S. Code stating that DoD-appropriated funds may not be used for any training, equipment, or other assistance for a foreign security force unit if the Secretary of Defense has credible information that such unit has committed a GVHR. The law allows for an exception to this restriction in cases where the Secretary of Defense (after consultation with the Secretary of State) determines that the government of that country has taken all necessary corrective steps. Additionally, exceptions are permitted if U.S. equipment or other assistance is necessary to assist in disaster relief operations or other humanitarian or national security emergencies.

4.5 UN Security Council Consolidated Sanctions List

The Consolidated Sanctions List includes all individuals and entities subject to sanctions measures imposed by the U.N. Security Council. Each sanctions committee established by the U.N. Security Council therefore publishes the names of individuals and entities listed in relation to that committee as well as information concerning the specific measures that apply to each listed name.
https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

4.6 OFAC Compliance

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the U.S.. While most contracts or cooperative agreements in which UNISHKA is involved are accompanied by OFAC license, there are occasions when the scope of the license is insufficient to address expanded work under the agreement and an new or amended OFAC license is required. Specifically, UNISHKA often assists anti-corruption groups in procuring website domain names and web hosting, both specifically prohibitted by 31 C.F.R. 540 (b)(4). In those instances, requests to issue a new license or expand an existing license should be sent through the contracting government agency to OFAC (see Addendum 1).

4.7 ITAR Compliance

International Traffic in Arms Regulations (ITAR) was developed originally to regulate military products and services. As technology has grown, the scope of ITAR coverage has also expanded to include commercial products such as electronics, computers, hardware and software. The ITAR applies even when the US Government (i.e. DoS, DoD) is the client. If in the performance of a contract for a U.S. government agency UNISHKA discloses controlled technical data or software to a foreign party or performs a regulated service for a foreign party, it may be required to obtain an export license or enter into a Technical Assistance Agreement (TAA). If an ITAR exemption is provided in a government contract or cooperative agreement, UNISHKA must maintain those records for not less than 5 years, in accordance with CFR §123.26.

5 UNISHKA VETTING POLICY

It is the policy of UNISHKA to screen individuals and business entities with whom it has a pecuniary or non-pecuniary relationship in order to mitigate the risk that it could inadvertently provide support to entities or individuals deemed to be a risk to national security in contravention of established law. The procedure by which this screening occurs is called the UNISHKA Vetting Process.

6 UNISHKA VETTING PROCESS

Application of UNISHKA's vetting process is mandatory for the following:

- Employees, consultants, interns, vendors, sub-contractors, grantees and sub-grantees who work on projects, receive funds or receive benefits under any project supported in anyway by appropriated funds of DoS or DoD.
- Any individual or other entity who is receiving funds or benefits from UNISHKA and who has traveled to or resided in any country identified on any DoS *Country Reports on Terrorism*.
- Employees, consultants, interns, vendors, sub-contractors, grantees, sub-grantees and individuals or entities receiving funds or benefits from UNISHKA where, under the totality of circumstances, there is a reasonable risk that UNISHKA could inadvertently provide support to entities or individuals deemed to be a risk to national security in contravention of established law.

The vetting process begins with the collection of identifying information. For individuals, this usually requires the completion of a UNISHKA Vetting Form (see Addendum 2). In addition, a copy of the applicant's passport and CV should also be collected whenever possible.

Identifying information concerning an applicant should be kept on a secure platform, such as the UNISHKA Portal. Copies of the applicant's identifying information received on unsecure platforms (such as Gmail, Yahoo or similar email providers) should be completely deleted and removed from the platform's "trash." When emailing an applicant's identifying information, it is required to use UNISHKA's encryption subscription service (Barracuda) when operating outside of the Microsoft 365 platform.

Vetting must be renewed annually for projects using appropriated funds of DoS or DoD. For other individuals and entities for whom the vetting process is mandatory, vetting must be initiated at the beginning of each

project and intermittently thereafter, as is reasonable and prudent to mitigate risk.

For U.S. government-funded projects, the identifying information should be sent directly (or through a prime contractor) to the designated government agency (e.g. DoS) for screening.

For privately funded projects, it is UNISHKA policy to submit identifying information to a Third Party Vendor to ensure compliance. If the client has a third-party vendor, such as eCustoms (i.e. Visual Compliance), this will suffice for UNISHKA's Third Party Vendor. If the client does not have a Third Party Vendor, then UNISHKA should contract for screening services with a Third Party Vendor to ensure compliance.

No funds or benefits of value should be expended on any applicant until an affirmative screening determination has been received.

7 INTERIM VETTING PROCESS

It is UNISHKA's responsibility to ensure that all persons working on specifically enumerated projects have been vetted. "Interim vetting" is not in the written policies of DoS but is incorporated into their working guidance (see Addendum 4: Email from Christopher B. Taylor dated 4/19/2016). In short, if an individual has been vetted on another project, they are "interim vetted" for subsequent projects subject to the following process:

- UNISHKA must collect the applicants identifying information (i.e. Vetting Form, Passport);
- The applicant must be successfully submitted for vetting under the current project;
- UNISHKA must confirm from the previous project that the applicant was successfully vetted under that project;
- An Interim Vetting Request must be sent through channels to the current GOR as well as the GOR for the previous project requesting interim vetting (see Addendum 3);
- An Interim Vetting Approval email will be sent from the current GOR and should be kept pending full vetting; and,
- Interim Vetting will allow the integration of an applicant into the project pending successful inclusion on a Vetting Evaluation List.

ADDENDUM 1: OFAC SAMPLE LICENSE REQUEST

27 May 2014 Applicant Reference Identification: URS-060114-01

U.S. Department of Treasury
Office of Foreign Asset Control
Washington D.C. 20220

Subject: Request for License to Acquire Domain Name Registration Services and Web Hosting Services for Persons Covered Under 31 C.F.R. 501, 540 et. seq.

Applicants: UNISHKA Research Service, P.O. Box 240241 Douglas, Alaska 99824

Dear Sir or Madam:

Under Solicitation SOL-OAA-12-xxxxx The Big Company (TBC) administers a project entitled TOGAR (the TOGAR Project). TBC subsequently subcontracted portions the technical implementation of the solicitation to UNISHKA Research Service.

In the administration of the project, UNISHKA has conducted several anti-corruption seminars and study tours with graduate and post-graduate students as well as activists and academics from Afghanistan, Iraq, Iran, Pakistan, Tajikistan and Kyrgyzstan. All of these participants are vetted through the RAM system.

During these seminars, participants are encouraged to create work plans that promote anti-corruption activities and the dissemination of information concerning both corruption and anti-corruption in their home countries.

Two of the current participants would like to create a website or sites where academic papers concerning corruption and anti-corruption that have been translated from English can be published for public review and comment. To ensure the sanctity and continuity of the website(s), the participants believe that it would be beneficial to host the website(s) on a server located outside of their home country. Consequently, at one of the anti-corruption training seminars they requested UNISHKA to purchase domain name registration services and web hosting services to facilitate this initiative.

To fulfill this request without an OFAC license appears to be in contravention of the applicable regulations. 31 C.F.R. 540 (b)(4) reads in part:

This section does not authorize: The direct or indirect exportation of web-hosting services that are for purposes other than personal communications (e.g., web-hosting services for commercial endeavors) or of domain name registration services.

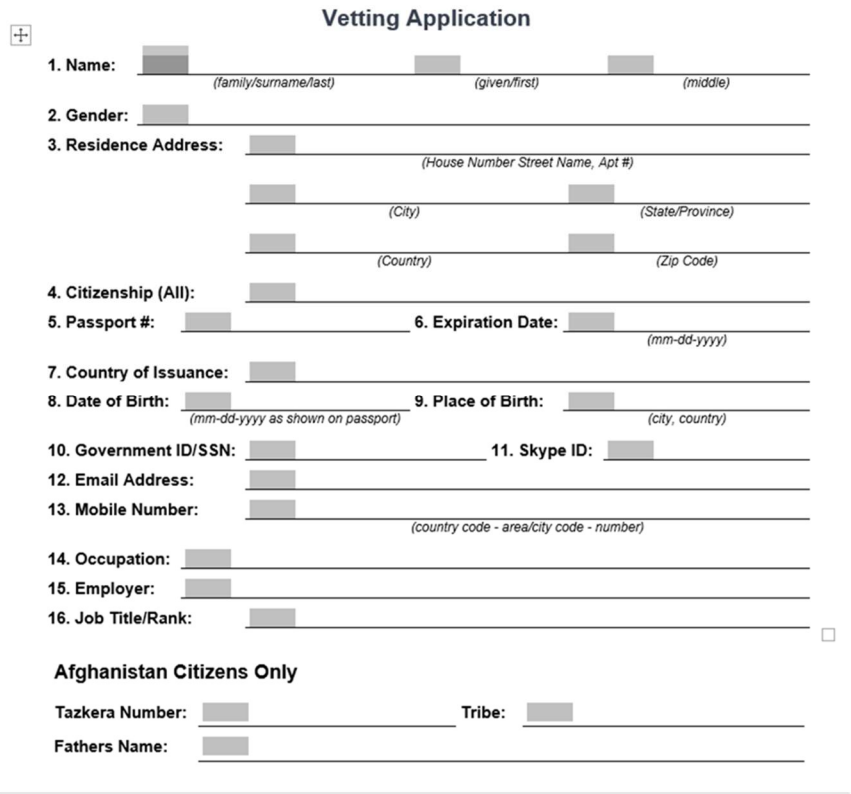
Furthermore, in General License D-1 dated 7 February 2014, it states that the "exportation or re-exportation, directly or indirectly, of web-hosting services that are for commercial endeavors or of domain name registration services" are not authorized.

The proposed web-hosting services that are the subject of this request are not for commercial purposes but are for 'other than personal communications' (*i.e.* the dissemination of anti-corruption material). Consequently, acquisition and exportation of the proposed web-hosting services appears to be in contravention of the applicable regulations. Additionally, acquiring domain name registration services for exportation also appears to be in contravention of the applicable regulations.

Therefore, on behalf of the Applicant(s), I request that a license be granted to procure domain name registration services and web-hosting services for the individuals identified at Addendum 1 in order to facilitate anti-corruption activities. The proposed transaction envisions that the Applicant(s) purchase domain name registration services and web-hosting services on behalf of the covered foreign nationals from a commercial vendor. These services will then be transferred to the foreign nationals so that they might construct a website dedicated to anti-corruption activities in their native language.

The point of contact for this action is Jeffrey Coonjohn, jjcoonjohn@unishka.com.

ADDENDUM 2: UNISHKA VETTING FORM



Vetting Application

1. Name: _____ _____ _____
(family/surname/last) (given/first) (middle)

2. Gender: _____

3. Residence Address: _____
(House Number Street Name, Apt #)

_____ _____
(City) (State/Province)

_____ _____
(Country) (Zip Code)

4. Citizenship (All): _____

5. Passport #: _____ 6. Expiration Date: _____
(mm-dd-yyyy)

7. Country of Issuance: _____

8. Date of Birth: _____ 9. Place of Birth: _____
(mm-dd-yyyy as shown on passport) (city, country)

10. Government ID/SSN: _____ 11. Skype ID: _____

12. Email Address: _____

13. Mobile Number: _____
(country code - area/city code - number)

14. Occupation: _____

15. Employer: _____

16. Job Title/Rank: _____

Afghanistan Citizens Only

Tazkera Number: _____ Tribe: _____

Fathers Name: _____

ADDENDUM 3: SAMPLE INTERIM VETTING REQUEST

September 15, 2017

From: Chris Jeffries, Project Manager, TOBUS Project, UNISHKA Research Service

To: Taylor Christie, Department of State, Bureau of Near Eastern Affairs, Office of Assistance Coordination

Subject: TOBUS Project - Interim Vetting Request for Ahmad Mohammedi

REF: S-NEAAC-17-CA-1372 – UNISHKA – TOBUS

Summary:

The TOBUS project works with journalists, attorneys and social advocates in the field of anti-corruption in the Middle East and Central Asia. Consequently, secure communications and secure information platforms are imperative to the success of the program as well as the security of our participants. UNISHKA is undergoing a Cyber Security Audit to ensure its communications, information platforms and processes provide robust security for both the project and its participants.

The Cyber Security Audit is being conducted by A-1 Technologies, Inc. of Cheeseport, Wisconsin. The President of A-1 is Mr. Ahmad Mohammedi. Mr. Mohammedi recently conducted a similar audit for TrueNews under a sub-grant from RTI. Consequently, Mr. Mohammedi and his team were vetted by RTI (per Ms. Rebecca Jones). Mr. Mohammedi has been submitted for vetting under the TOBUS project. Based upon his previous vetting under the RTI project, however, we are requesting *interim vetting* for Mr. Mohammedi so that A-1 can conclude the UNISHKA Cyber Security Audit on schedule.

Please let me know if you have any additional questions or concerns. I can be reached on my mobile phone at 202-867-5309.


UNISHKA
Research Service