Export Controls and National Security (RCR)

Content Authors

- **Mary M. Beran, MA, CPIA**
  Georgia Institute of Technology
- **Daniel A. Vallero, PhD**
  Duke University

Introduction

No single source can capture all of the complexities inherent to research security as it relates to U.S. export control regulations. The hacking of the U.S. Office of Personnel Management provides a clear example of what is at stake when cyberattacks or other unauthorized access is gained. In this case, the breach included identifying and other important information from the security clearance applications of over 20 million people and another 2 million non-applicants (for example, spouses and partners of applicants).

Complicating modern research is that various workplaces have unique requirements. The basis for the variety of requirements is the protection of the welfare, stability, and security of the United States. Regulatory security requirements may take the form of a government issued security clearance (for example, access to data that are Classified at Top Secret) whereby an individual is issued the clearance only after an extensive background check. Security requirements may also take the form of contract clauses used to enforce federal regulations. However, even when contract terms do not specify export control requirements, the individual is still held responsible and accountable for any information, material, or technology that is exported or shared with a foreign national.

This module introduces major elements related to export control, particularly as they fit the broader focus of responsible conduct of research. However, learners who need to receive more comprehensive training on the topic should refer to the CITI Program's Export Control (EC) series. This module is for educational purposes only. **IT IS NOT** designed to provide legal advice or legal guidance. Please consult with your organization's export control office or attorneys if you have questions about the relevant laws and regulations discussed in this module.

By the end of this module, you should be able to:

- Discuss the importance of research to national security.
- Define Fundamental Research.
- Describe the Fundamental Research Exclusion and how it applies to a research program.
- Discuss what a Technology Control Plan (TCP) is and how it relates to International Traffic and Arms Regulations (ITAR), Export Administration Regulations (EAR), and Fundamental Research.
- Define what an Export and Deemed Export are in the regulatory context.
- Provide examples of different types of research with potential security or export control implications.
- Explain difficulties related to upholding cybersecurity.
- Discuss issues surrounding international travel and shipping concerns.

The Importance of Research to National Security

After the September 11, 2001 terrorist attacks on the U.S., homeland security became a matter of increasing concern. The Patriot Act and the Improving America's Security Act of 2007, also known as the 9/11 Bill, are examples of the government's attempt to protect the country. Examination of publicly available information led to pressures to restrict publication of certain types of new technologies and scientific research. For example, an Assistant Secretary of the U.S. Department of Health and Human Services attempted to edit a paper and remove sensitive information prior to its publication in the *Proceedings of the National Academy of Sciences* (PNAS); the paper described a hypothetical scenario where *botulinum* toxin could be used to contaminate milk supplies (Alberts 2005).

At the 2003 annual meeting of the American Association for the Advancement of Science (AAAS), thirty-two science journal editors released a statement regarding the potential risks of publishing research results that could be manipulated to cause harm (Shea 2006). In 2004, a National Academy of Sciences (NAS) committee expressed the concern that "publication of research results provides the vehicle of the widest dissemination, including to those who would misuse them" (NRC 2004a). Additionally, the terrorist attacks and the distribution of anthrax spores through the mail in 2001 have caused increased scrutiny of nonconventional weapons. A series of publications, including one indicating that the polio virus could be created artificially (Shea 2006) and others about the bird-flu virus (Collins 2012), escalated concerns over whether publishing research results could threaten national security.

The U.S. government has historically supported the open publication of federally funded research results unless the award or contract contained a specific restriction, typically imposed by the funding agency in accordance with policies and directives "for controlling the flow of science, technology, and engineering information produced in federally-funded fundamental research at colleges, universities, and laboratories" (NSDDs 1985). In cases where results raise national security concerns, several mechanisms can be used. For advanced technology and technological information resulting from commercial and other non-federally sponsored fundamental and applied research, a combination of classification and regulations, including export and arms trafficking regulations, have been put in place to manage access.

Regulations & Definitions

In order to understand the export regulations, one must first know the definition of an export. An export can be many different things including the transfer or disclosure of items, materials, information, software, technology, or other unclassified but restricted data to any person outside the U.S. (including U.S. citizens abroad). The U.S. Department of State considers defense services to be exports.

Deemed Exports

"A further complication to export regulation is the concept of a 'deemed export.' A deemed export is transfer of information, not physical items, to a foreign national without first obtaining an export license for that technology. This provision has been especially troubling for universities, as foreign students and researchers who attend graduate-level classes may be exposed to information relating to technology which falls under export controls" (Shea 2006).

Without a license from the U.S. Department of State, foreign persons (including graduate students) may not come into contact with export controlled information. This means that even in the same department or laboratory, the supervisor, manager, principal investigator, or other responsible person is obliged to protect this information from improper release, even if it would be technically efficient and advantageous to share it with students and colleagues who are prohibited by law to have it.

To appreciate how relevant federal regulations might affect research, one must first understand the meaning of "fundamental research".

Fundamental Research

Federal policy, as described in National Security Decision Directive 189, holds that fundamental research should remain unrestricted in most cases. However, when it is necessary to restrict such information, the appropriate vehicle is "classification". NSDD-189 (1985) states:

> 'Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

Much of the research that is ordinarily performed at a university is covered under the Fundamental Research Exclusion (FRE). The FRE applies to:

- Information (not including items or materials) resulting from or arising during basic and applied research in science and engineering
- Conducted at an accredited institution of "higher education" (EAR) or "higher learning" (ITAR)
- Located in the U.S. (does not apply abroad)
- Resulting information that is ordinarily published and shared broadly in the scientific community and
- Is not subject to proprietary or U.S. government publication or access dissemination controls (for example, a restriction on foreign national participation (22 C.F.R. 120.11(8); 15 C.F.R. 734.8(a) and (b))

An organization that accepts a grant or contract with access or dissemination controls or restrictions may no longer use the FRE on that specific project or award. Academic institutions confront a variety of situations with sponsors that can restrict their ability to disseminate research results (AAU/COGR 2008). If the project involves export-controlled data, it clearly would not be eligible for the FRE. However, a common contract clause that has a significant impact on the export control status of a research programs is the Publication Restriction DFARS (2013) 252.204-7000 clause, which is better known as the "7000 clause":

> The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of the medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract.

There are exceptions delineated in the "7000 clause"; yet in general, it has a second-order effect in that the project is no longer conducted under the FRE from export controls (AAU/COGR 2008).

Restrictions Imposed By Sponsors

A publication restriction such as the 7000 clause (**DFARS 252.204-7000**) may be used on research contracts where the sponsor does not want information disseminated or released. There can be several reasons for this prohibition. An example related to a national security issue is an unclassified project that investigates weaknesses in the security at major airports. While the results of the study are unclassified, the government sponsor may not want these security weaknesses to be published.

Genome research limitations, described in a National Academies report (NRC 2004b), provide another example:

> In an ideal world, it would be easy to advocate for a free and ready distribution of all genome information into the public domain. That would be in the spirit of free scientific inquiry as it would lead to the most scholarly and creative use of the information that is inherent (although not always obvious) in the deciphering of the genomic blueprint of any living thing. However, we live in a world where a small minority of individuals and, sadly, perhaps even some world governments might use pathogenic microbes as weapons. We have to ask to what extent genomic information, particularly of microorganisms and their hosts, might help these misguided individuals.

Once a project falls outside of the FRE, it is subject to the export control regulations described below.

ITAR, EAR and OFAC

Federal regulations restrict international information flow. These regulations include the Export Administration Regulations (EAR) under the U.S. Department of Commerce and the International Traffic in Arms Regulations (ITAR) under the U.S. Department of State. The EAR controls the export and re-export of commercial goods and technology, including dual use items (described below).

ITAR regulates items on the Department of State's Munitions Control List, typically defense articles (including space related) and the associated technical information. While some items are clearly developed for a commercial use and other items are clearly developed for a military use, researchers can easily find themselves working in an area that has both commercial and military applications.

A colleague in a foreign country has been working with Dr. Thomas on a Department of Defense (DoD) contract to design a facemask to protect individuals from different forms of gases. They have come up with a new design that they feel confident will work with a number of different gasses. The DoD sponsor wants them to test it with Diphenylchloroarsine, a toxic gas that is rarely lethal and then only in extremely high concentrations. Only the colleague in the foreign country has the equipment to test the mask but does not have access to the Diphenylchloroarsine.

Is Dr. Thomas allowed to send the Diphenylchloroarsine to a colleague for testing with the mask if the DoD sponsor approves?

In addition to the EAR (Commerce) and ITAR (State) that regulate specific items and goods, the Office of Foreign Assets Control (OFAC) under the U.S. Department of Treasury regulates economic and trade sanctions based on foreign policy and national security goals. OFAC sanction programs are targeted to address issues with 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 United States. When establishing a research collaboration or otherwise working with an embargoed country, such as Iran, North Korea, or Syria, a license will be required.

Dr. Jones is taking a group of students from his art history class on a one week trip to the Sudan. His plan is to take a laptop and a GPS for use in the event that he gets lost. While there, he plans to buy a few pieces of art from his favorite Sudanese artist and his students are likely to do the same. His students will likely want to take their mobile electronic devices with them as well.

Are there any export concerns?

Dual Use

A standard definition of dual use is a technology that can be used for both commercial and military aims. Dual use items are controlled under the EAR by the U.S. Department of Commerce and enforced by its Bureau of Industry & Security (BIS). In general, a significant problem with dual use technology is that one person's military use is another person's civil use.

An example of a dual use technology is a nuclear reactor. A nuclear reactor can generate clean energy for sale to consumers everywhere (civil use). However, the by-product material in the reactor, after the energy is generated, is plutonium; this can potentially be refined for developing an atomic bomb. Thus, a country wishing to develop a nuclear program may decide to build a nuclear reactor under the pretense that it is intended for civil use when the actual purpose is to create nuclear weapons.

Computers provide another example of dual use technology. Historically, the sale of U.S. made laptops to the Soviet Union/Russia has been publicly criticized since it was suspected that computers were being transferred to the military and weapon design laboratories to be disassembled and used for military purposes.

Also, as Jay Stowosky (1996, 56-64) suggests, "policy makers were concerned that if the United States let foreign firms take the lead in the commercial development of dual-use technologies, the Pentagon could ultimately become dependent on foreign suppliers for key military components."

Dual Use Case Study

A growing concern for research communities is the application of the life sciences. For example, genetic engineering has real and potential value, but it can also introduce threats to public health and safety. The potential for weaponized microbes and other bioterrorism agents is a particularly daunting dual use. The concern has grown, highlighted by the publication of manuscripts related to the enhanced transmissibility of the H5N1 highly pathogenic avian influenza virus (Imperiale and Casadevall 2015). The U.S. Government's **Policy for Institutional Oversight of Life Science Dual Use Research of Concern**, effective September 24, 2015, describes practices and procedures related to research that could introduce such risks. Dual use research of concern is a subset of dual use research defined as:

> life sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, materiel, or national security (HHS 2015)

Professional and research due diligence requires that one consider the possible good and bad outcomes of a project. Protections need to be in place even for a worthwhile biotechnology in order to prevent misuse, now and down the road. This certainly applies to research that can raise bioterrorism concerns (for example, work involving pathogens); but it also applies to research that has more subtle vulnerability (for example, synthetic biology and biomaterials for pharmaceutical and agricultural purposes). In the latter case, it may well call for greater imagination and longer time horizons to identify adverse outcomes.

The Importance of Technology

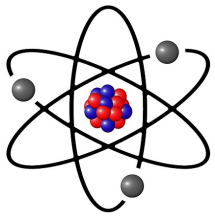
The economy of the United States is based in large part on the commercialization of scientific and engineering accomplishments such as aircrafts, computers, energy generation, and medical devices. One might think that leaps in technological achievements are rather new. However, as evident in the Science The Endless Frontier (Bush 1945), the focus on innovation and the utilization of innovative technologies has been a topic for quite some time. Technological achievements are spreading across the globe. The Defense Science Board 2006 Summer Study (2007) entitled 21st Century Strategic Technology Vectors explains that the US has been displaced in its lead on some militarily relevant technologies by international commercial industries and markets.

A committee of the National Academy of Sciences (NAS 2007) produced an influential report entitled *Rising Above The Gathering Storm* that included the following section:

> Having reviewed trends in the United States and abroad, the committee is deeply concerned that the scientific and technical building blocks of our economic leadership are eroding at a time when many other nations are gathering strength. We strongly believe that a worldwide strengthening will benefit the world's economy - particularly in the creation of jobs in countries that are far less well-off than the United States. But we are worried about the future prosperity of the United States. Although many people assume that the United States will always be a world leader in science and technology, this may not continue to be the case inasmuch as great minds and ideas exist throughout the world. We fear the abruptness with which a lead in science and technology can be lost - and the difficulty of recovering a lead once lost, if indeed it can be regained at all.

Researchers can contribute to the public good in many different ways. Some can contribute by creating new technologies for use in the medical fields that will result increasing survival rates for injured or ill patients. Others will contribute new advances in defense related technology to strengthen and protect the military.

Ethical Challenges



Researchers can confront ethical challenges related to the public's unease about technological developments, such as electrical systems, airplanes, and nuclear reactors. In some cases, researchers should clarify how the technology is going to be used, and they should aim to incorporate safety features to prevent misuse. Issues may also emerge related to questions of morality such as working (or not working) on defenses against chemical, biological, or nuclear weapons, and working for or as defense contractors. Not all ethical challenges are obvious. For example, there are many improvements in the areas of engines, tires, mapping, communications, miniaturization, and nanotechnology. Each new development or improvement can lead to a better, more efficient use of the specific technology. However, any one of these technologies can be used for good or malicious purposes.

Research results can be surprising and some applications can be misguided. For example, Carl Djerassi (1990) developed steroids for use in rehabilitating patients whose muscles had atrophied in recovering from extensive injuries. However, steroids are now widely used, at times illegally, to enhance athletic performance.

Should researchers refuse to undertake a project if they think it might have a misguided result? This is not an easy question to answer. Here is one view from a NAS member quoted in a Sigma Xi booklet (1999, 54):

> I object strenuously to the concept of the social responsibility of science. I think this is an incongruous idea. I think science ought to be value free. People should be concerned about how the science is used in pursuit of societal goals, but I don't want the scientist to be responsible for worrying about the outcome of his science for the public at large.

In response, another NAS member states:

> The statement concerning social responsibility of science is pure rot. We all have a responsibility to act according to our beliefs, and to avoid actions we feel to be evil. We cannot enforce the proper behavior of others, but we can certainly do so for ourselves.

There are many related questions to consider. For example, should concerns about the public's welfare or national security determine whether, and where, research is conducted? What kinds of ethical considerations should a researcher take into account when deciding whether to work on nuclear weapons or their delivery systems? What is the decision process for deciding if a researcher can work on conventional weapons? Individual researchers and research communities need to reflect on which values are appropriate to uphold.

Classified Work

Classification is one of the key measures that can be taken to protect and control information. However, classified research and regulations are not the same as export controlled research and regulations. Some institutions do not allow classified work to be conducted on their campuses. Others welcome it and contract with special facilities that ensure all applicable and necessary security measures are taken. Some institutions who engage in classified research have set up or contracted with affiliated laboratories or organizations to separate or isolate the classified work from the work performed across the rest of the institution.

Cybersecurity

The U.S. government has tightened physical security at its facilities and the Nuclear Regulatory Commission has done the same for nuclear power plants. However, most researchers are more likely to be involved in activities where another type of security is crucially important - **cybersecurity**.

The Internet has numerous security vulnerabilities. Anything one does on a computer can likely be accessed by others. One should expect that anything sent via the Internet can potentially be intercepted by others besides the intended recipient. Because viruses can enable one's computer to be taken over, the latest version of anti-virus software should be installed. That may help to prevent many intrusions. However, a sophisticated attacker can still get into a computer so proprietary, sensitive, and export controlled material must be handled in a careful manner. The **only** guaranteed firewall is an air-gap (in other words, no connection between the computer and the external world).

In addition to dishonest intrusion, it is important to realize that anything done on the Internet can be considered an international action for the purpose of export controls. As high-profile hacking incidents indicate, the need for vigilance about cybersecurity continues to

grow.

Collaborating with Foreign Researchers and Students

Working with foreign nationals in laboratories and transferring of information overseas can raise export concerns. What are the boundaries and guidelines? When and in what manner is it acceptable to share information with citizens of those countries?

Case Study Professor Smith is giving a presentation on the development of a new algorithm (which is projected to have significant use in encryption technology) to an advanced mathematics class that includes an exchange student from a foreign country.

What are the export control ramifications?

The definition of a **Foreign Person** is different under the export control regulations than under the classified regulations. Foreign persons under the export control regulations are those who are not permanent lawful U.S. residents. Individuals with U.S. citizenship, Green Card, or documented Political Asylum are considered U.S. persons under the EAR and ITAR. However, when working on classified projects, Green Card Holders/U.S. Permanent Residents are considered Foreign Persons under National Industrial Security Operating Manual (NISPOM).

Researchers can collaborate on projects that are eligible for FRE. However, if a project contains export controlled information, access, or dissemination controls or restrictions as previously discussed, a license may be required to involve foreign collaborators.

Access Control

Allowing access to information or materials is not only determined by nationality. A number of individuals, U.S. citizens and non-US-citizens, **are placed on lists that prohibit them from receiving federal funds or other assistance**.

Being on one of these lists can also prohibit others from entering into other types of dealings with these individuals.

It is important to note that "The USA PATRIOT Act…created another mechanism to block certain foreign nationals from obtaining specific information. Access to or information about biological and toxic agents on the 'select agent' list is barred to individuals, including students, originating from countries which support terrorism" (Shea 2006).

Additionally, foreign collaborators from embargoed countries (including Iran, North Korea, Sudan, and Syria) may only have access to FRE projects and they cannot have access to any export restricted projects without a license.

The Researcher's Role in Protection - Technology Control Plans

The researcher as part of being involved in and overseeing export controlled research plays a crucial role in ensuring security. Safeguards such as a Technology Control Plan (TCP) can be put in place to protect against inadvertent release of export controlled information.

A TCP should include the following elements:

- Commitment
- Physical Security
- Information Security
- Personnel Screening
- Training and Awareness
- Self-Evaluation

A TCP should be a living document. It should be modified as needed to protect the research program.

The TCP begins with awareness of the possibility that certain items and information may require clearance, a license, or at least certain prescribed and/or special protections. The next step is obtaining the necessary knowledge to make a decision regarding the levels of security that must be considered and applied when working with such items and information. The researcher must know about the obligations that are created relating to the ownership of the information and the protections that are needed.

The researcher may need to implement behavioral and practical changes in response to new knowledge and make decisions accordingly. For example, some information is so sensitive that sharing it with anyone who lacks the appropriate security clearance and need-to-know (classified materials) or with a foreign national (export-controlled material) without the appropriate clearance and need-to-know or export license could result in criminal charges being filed against one or more of the involved parties.

In addition to understanding how and where export controlled information should be handled and stored, working on an export controlled project can influence travel plans. Export controlled data may not be taken outside the U.S. without a license even if the data are encrypted on a laptop computer or other device. In fact, the level of encryption itself as well as the computer hardware may be controlled to the traveler's destination.

Case Study Dr. Adams is taking a group of students from her art history class on a one week trip to Europe. Her plan is to take a laptop and a GPS for use in the event that she gets lost. While there, she plans to buy a few pieces of art from her favorite European artist and her students are likely to do the same. Her students will likely want to take their portable music devices with them as well.

Are there any export concerns?

The researcher must evaluate the unique circumstances associated with each case. Charges against an individual and/or an organization could be civil or criminal depending on the details and circumstances of each case, including whether release of protected or controlled items and/or information was inadvertent or intentional. This and many other types of information breaches could certainly put the researcher's reputation, project, and career in jeopardy. Likewise, the organization can also receive penalties or even lose export privileges.

Individuals working on an export controlled program must have proper training to ensure that they fully understand the relevant requirements. The training should be broad enough to make sure that researchers recognize when they have confronted a situation where they might have to seek additional professional advice. Refer to the **U.S. Department of Commerce's BIS website** and one's organizational export website for more details.

Violations & Penalties

Researchers accepting awards or contracts that are export controlled must be aware that the acceptance of controlled projects brings with it significant responsibilities. Failure to comply with U.S. export control laws can result in severe penalties, both for the individual personally and for the organization. Criminal penalties can include fines of $1,000,000 per violation and imprisonment of up to 10 years. Civil penalties can include fines of $250,000 per violation, or twice the monetary amount of the underlying transaction, whichever is greater under EAR or $500,000 per violation under ITAR. ITAR, EAR, and OFAC all impose criminal and civil penalties, although the ranges of the penalties vary. In addition to significant fines and jail time, not being allowed to work with export controlled information and negative publicity can have a significant impact on a research program.

Academics have come to realize that there are penalties associated with violating federal regulations. A prosecution and subsequent conviction in a university setting for the transfer of controlled defense technology to foreign national graduate students came to light with the case of Dr. J. Reece Roth. Roth, a retired University of Tennessee professor, gained much attention in 2008 when he was sentenced to four years in prison for illegally exporting technical information, known as "technical data". The case related to Roth's disclosure and transport of restricted military information associated with a U.S. Air Force (USAF) contract to develop specialized plasma technology for use on an advanced form of an unmanned aerial vehicle (UAV), also commonly known as a drone (OPA 2009). **A Supreme Court brief about the case can be viewed here**.

Summary

In the United States, several federal regulations apply and must be considered when conducting research and other projects with foreign nationals and with researchers in other countries. While these regulations will not constrain most research activities, when in doubt, researchers should consult with an expert, such as a compliance officer, a lawyer, or an administrative official who is familiar with the application of export or other related regulations.

Acknowledgements

The authors would like to thank John F. Ahearne for his contributions to this module. The authors also appreciate the helpful comments offered by the anonymous reviewers.

References

- AAU/COGR Task Force. 2008. "**Restrictions on Research Awards: Troublesome Clauses 2007/2008**." Accessed August 17, 2015.
- Alberts, Bruce. 2005. "Modeling Attacks on the Food Supply." *Proceedings of the National Academy of Sciences* 102(28):9737-8.
- Bush, Vannevar. 1945. "**Science The Endless Frontier: A Report to the President by Vannevar Bush, Director of the Office of Scientific Research and Development, July 1945**." Washington, DC: United States Government Printing Office. Accessed August 17, 2015.
- Collins, Francis S. 2012. "**Statement by NIH Director Francis Collins, M.D., Ph.D. on the NSABB Review of Revised H5N1 Manuscripts**." Accessed August 17, 2015.
- Defense Federal Acquisition Regulation Supplement (DFARS). 2013. "**252.204-7000 Disclosure of Information**." Accessed August 17, 2015.
- Defense Science Board 2006 Summer Study. 2007. "**21st Century Strategic Technology Vectors**." Accessed August 17, 2015.
- Djerassi, Carl. 1990. *Carl Djerassi: Steroids Made it Possible*. American Chemical Society.
- Imperiale, Michael J., and Arturo Casadevall. 2015. "A New Synthesis for Dual Use Research of Concern." *PLOS Medicine*: e1001813.
- Institute of Medicine, National Academy of Sciences, and National Academy of Engineering. 2007. *Rising Above the Gathering Storm*. Washington, DC: The National Academies Press.
- National Research Council (NRC). 2004a. *Biotechnology Research in an Age of Terrorism*. Washington, DC: National Academies Press.
- National Research Council (NRC). 2004b. *Seeking Security: Pathogens, Open Access, and Genome Databases*. Washington, DC: The National Academies Press.
- National Security Decision Directives (NSDDs). 1985. "**NSDD-189: National Policy on the Transfer of Scientific, Technical and Engineering Information**." Accessed August 17, 2015.
- Shea, Dana A. 2006. "**Balancing Scientific Publications and National Security Concerns: Issues for Congress**." *CRS Report for Congress*. Accessed August 17, 2015.
- Sigma Xi. 1999. *The Responsible Researcher: Paths and Pitfalls*. Research Triangle Park, NC: Sigma Xi.
- Stowosky, Jay. 1996. "The Dual-Use Dilemma." *Issues in Science and Technology* 13(2):56-64.

- U.S. Department of Health and Human Services (HHS). 2015. Public Health Emergency. "**United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern**." Accessed August 4, 2015.
- U.S. Department of Justice, Office of Public Affairs (OPA). 2009. "**Retired University Professor Sentenced to Four Years in Prison for Arms Export Violations Involving Citizen of China**." Accessed August 17, 2015.
- U.S. Department of the Treasury. "**Office of Foreign Assets Control (OFAC)**." Accessed August 17, 2015.

Additional Resources

- Council on Governmental Relations (COGR). "**Publications - Export Controls**." Accessed August 17, 2015.
- National Research Council (NRC). 2005. *Effects of Nuclear Earth-Penetrator and Other Weapons*. Washington, DC: The National Academies Press.
- National Research Council (NRC). 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, DC: The National Academies Press.
- National Research Council (NRC). 2007. *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities*. Washington, DC: The National Academies Press.
- U.S. Department of Commerce. "**Export Administration Regulations (EAR)**." Accessed August 17, 2015.
- U.S. Department of State. "**International Traffic in Arms Regulations (ITAR)**." Accessed August 17, 2015.
- U.S. Government Accountability Office. 2007. "**Critical Infrastructure; Challenges Remain in Protecting Key Sector GAO-07-626T**." Accessed August 17, 2015.
- U.S. Government Accountability Office. 2006. "**Homeland Security: Guidance and Standards are Needed on Measuring the Effectiveness of Agencies' Facilities Protection Efforts GAO-06-612**." Accessed August 17, 2015.
- U.S. Government Accountability Office. 2006. "**Risk Management: Further Refinement Needed to Assess Risks and Protective Measures at Ports and Other Critical Infrastructure GAO-06-91**." Accessed August 17, 2015.
- Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (**USA Patriot Act**) Act Of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). Accessed August 17, 2015.
- World Association of Medical Editors (WAME). 2004. "**Policy Statement on Geopolitical Intrusion on Editorial Decisions**." Accessed August 17, 2015.

Original Release: April 2012
Last Updated: August 2015

Take the quiz for Export Controls and National Security (RCR)
Return to the module list for this course