Engineering Ethics—Case Studies in Espionage

by

Mark Rossow, PhD, PE

Introduction

The purpose of this course is to widen the professional engineer's understanding of engineering ethics through consideration of three case studies. The studies are actual espionage cases that have been successfully prosecuted by agencies of the Federal government. Espionage was chosen as the subject of the case studies because it provides exposure to ethical situations which are important but probably unfamiliar to most PEs. The ethical aspects of the cases are developed by identifying the standards of conduct for engineers that were violated by the actions of the convicted engineers.

Table of Contents

Case No. 1

Maryland Nuclear Engineer and Wife Sentenced for Espionage-Related Offenses

November 9, 2022

Department of Justice

A Maryland man and his wife were sentenced today for conspiracy to communicate Restricted Data related to the design of nuclear-powered warships.

Jonathan Toebbe, 44, of Annapolis, was sentenced today to 232 months, over 19 years, of incarceration. His wife, Diana Toebbe, 46, was sentenced to 262 months, more than 21 years, of incarceration. The Toebbes pleaded guilty to the conspiracy in August 2022.

“The Toebbes conspired to sell restricted defense information that would place the lives of our men and women in uniform and the security of the United States at risk,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “The Department of Justice remains committed to protecting U.S. defense technology.”

“If not for the remarkable efforts of FBI agents, the sensitive data stolen by Mr. Toebbe could have ended up in the hands of an adversary of the United States and put the safety of our military and our nation at risk,” said U.S. Attorney William J. Ihlenfeld II for the Northern District of West Virginia. “The FBI keeps American citizens safe from enemies both foreign and domestic and this case is an excellent reminder of their important work.”

“These actions are a betrayal of trust, not only to the U.S. Government, but also to the American people,” said Assistant Director Alan E. Kohler Jr. of the FBI’s Counterintelligence Division. “All U.S. Government employees swear to support and defend the Constitution of the United States, and with that oath comes the obligation to protect sensitive information. Those entrusted with such grave responsibility must be held accountable if they violate their oath and betray their country. The investigation which led to today’s sentencing is a reminder that the FBI and our partners will continue to doggedly pursue those who betray their sworn oath and those who aid them.”

“The Toebbes were willing to compromise the security of the nation by selling information related to naval nuclear propulsion systems, they are now being held accountable for their actions,” said Special Agent in Charge Mike Nordwall of the FBI Pittsburgh Field Office. “The FBI and our federal partners have an unwavering commitment to protect U.S. secrets and will continue to aggressively investigate and expose espionage activities conducted on U.S. soil.”

“Naval nuclear engineer Jonathan Toebbe was entrusted with our nation’s critical secrets and, along with his wife Diana Toebbe, put the security of our country at risk for financial gain,” said U.S. Attorney Cindy Chung for the Western District of Pennsylvania. “Their serious criminal conduct betrayed and endangered the Department of the Navy’s loyal and selfless service members. The seriousness of the offense in this case cannot be overstated.”

“The Toebbes betrayed the American people and put our national security at significant risk when they selfishly attempted to sell highly sensitive information related to nuclear-powered warships for their own financial benefit,” said Special Agent in Charge Brice Miller of the Naval Criminal Investigative Service (NCIS) Office of Special Projects. “As the law enforcement arm of the Department of the Navy responsible for preventing terrorism, reducing crime, and protecting secrets, NCIS remains committed to protecting vital information and technology that ensures the superiority of the U.S. Navy and Marine Corps.”

According to court documents, at the time of his arrest, Jonathan Toebbe was an employee of the Department of the Navy who served as a nuclear engineer and was assigned to the Naval Nuclear Propulsion Program, also known as Naval Reactors. He held an active national security clearance through the Department of Defense, giving him access to “Restricted Data” within the meaning of the Atomic Energy Act. Restricted Data concerns design, manufacture or utilization of atomic weapons, or production of Special Nuclear Material (SNM), or use of SNM in the production of energy – such as naval reactors. Jonathan Toebbe worked with and had access to information concerning naval nuclear propulsion including information related to military sensitive design elements, operating parameters and performance characteristics of the reactors for nuclear powered warships.

According to court documents, Jonathan Toebbe sent a package to a foreign government, listing a return address in Pittsburgh, Pennsylvania, containing a sample of Restricted Data and instructions for establishing a covert relationship to purchase additional Restricted Data. Jonathan Toebbe began corresponding via encrypted email with an individual whom he believed to be a representative of the foreign government. The individual was really an undercover FBI agent. Jonathan Toebbe continued this correspondence for several months, which led to an agreement to sell Restricted Data in exchange for thousands of dollars in cryptocurrency.

On June 8, 2021, the undercover agent sent $10,000 in cryptocurrency to Jonathan Toebbe as “good faith” payment. Shortly afterwards, on June 26, Jonathan Toebbe serviced a dead drop by placing an SD card, which was concealed within half a peanut butter sandwich and contained military sensitive design elements relating to submarine nuclear reactors, at a pre-arranged location. After retrieving the SD card, the undercover agent sent Jonathan Toebbe a $20,000 cryptocurrency payment. In return, Jonathan Toebbe emailed the undercover agent a decryption key for the SD Card. A review of the SD card revealed that it contained Restricted Data related to submarine nuclear reactors. On Aug. 28, 2021, Jonathan Toebbe made another “dead drop” of an SD card in eastern Virginia, this time concealing the card in a chewing gum package. After making a payment to Jonathan Toebbe of $70,000 in cryptocurrency, the FBI received a decryption key for the card. It, too, contained Restricted Data related to submarine nuclear reactors. The FBI arrested Jonathan Toebbe and his wife on Oct. 9, 2021 after he placed yet another SD card at a pre-arranged “dead drop” at a second location in West Virginia.

The FBI and NCIS are investigating the case.

Trial Attorneys Matthew J. McKenzie and S. Derek Shugert of the National Security Division's Counterintelligence and Export Control Section, Assistant U.S. Attorneys Jarod J. Douglas and Lara Omps-Botteicher for the Northern District of West Virginia and Special Assistant U.S. Attorney Jessica Lieber Smolar for the Western District of Pennsylvania prosecuted the case.

Case No. 2

Navy Civilian Engineer Sentenced to 11 Years for Attempted Espionage

October 15, 2015

U.S. Department of Justice

WASHINGTON—Mostafa Ahmed Awwad, 36, of Yorktown, Virginia, was sentenced today to 132 months in prison by U.S. District Judge Raymond A. Jackson of the Eastern District of Virginia for attempted espionage relating to his attempt to provide schematics of the nuclear aircraft carrier USS Gerald R. Ford to Egypt while serving as a Navy engineer.

Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Dana J. Boente of the Eastern District of Virginia, Assistant Director Randall C. Coleman of the FBI's Counterintelligence Division and Special Agent in Charge Tim Quick of the Naval Criminal Investigative Service (NCIS) Norfolk, Virginia, Field Office made the announcement.

"Awwad took advantage of his position of trust within the Navy to share the schematics of the USS Gerald R. Ford nuclear aircraft carrier with individuals whom he believed were representing a foreign government," said Assistant Attorney General Carlin. "The National Security Division will continue to seek justice for those who abuse their access to sensitive defense information."

"Awwad attempted to steal the valuable plans for the USS Ford and to provide them to a foreign government," said U.S. Attorney Boente. "This office is committed to safeguarding our nation's sensitive defense information, and we will bring to justice those who seek to steal it. I want to commend our partners at the FBI Norfolk and NCIS Norfolk for their excellent work on this case."

"The mission of NCIS includes protecting Sailors and secrets," said Special Agent in Charge Quick. "Awwad endangered both; for personal gain and to help strengthen another nation's military. It's gratifying that NCIS was a part of bringing him to justice."

Awwad pleaded guilty on June 15, 2015. According to court documents, Awwad began working for the Department of the Navy in February 2014 as a civilian general engineer in the Nuclear Engineering and Planning Department at the Norfolk Naval Shipyard. Based on a joint investigation, an undercover FBI agent contacted Awwad by telephone on Sept. 18, 2014, and asked to meet him the following day. Without seeking additional information from the caller, Awwad agreed. The next day, Awwad met with the undercover FBI agent, who was posing as an Egyptian intelligence officer, in a park in Hampton, Virginia. During the meeting, Awwad claimed it was his intention to utilize his position with the U.S. Navy to obtain military technology for use by the Egyptian government, including but not limited to the designs of the USS Gerald R. Ford nuclear aircraft carrier, a new Navy "supercarrier." Awwad agreed to

conduct clandestine communications with the undercover FBI agent, and to conduct "dead drops" in a concealed location in the park.

On Oct. 9, 2014, Awwad and the undercover FBI agent met at a hotel where Awwad described a detailed plan to circumvent U.S. Navy computer security by installing software on his restricted computer system that would enable him to copy documents without causing a security alert. At this time, Awwad also provided the undercover FBI agent with four Computer Aided Drawings of a U.S. nuclear aircraft carrier downloaded from the Navy Nuclear Propulsion Information system. During the discussion, Awwad indicated his understanding that the drawings would be sent to and used in Egypt. Awwad also asked the undercover FBI agent for $1,500 to purchase a pinhole camera that he would wear around the shipyard to photograph restricted material. At the conclusion of the meeting, Awwad agreed to provide the undercover FBI agent with passport photos which would be used to produce a fraudulent Egyptian passport so that Awwad could travel to Egypt without alerting U.S. government officials.

On Oct. 23, 2014, Awwad traveled to the prearranged dead drop site situated on a secluded hiking trail and utilized a concealed container disguised in a hole in the ground. He retrieved $3,000 before placing an external hard drive and two passport photos inside.

On Dec. 5, 2014, Awwad and the undercover agent met in the Hampton Roads, Virginia, area. During this meeting, Awwad stated that he planned to travel to Egypt. Awwad subsequently said he wanted to meet with "high ranking" Egyptian intelligence and military officials in Cairo. Awwad also stated during the meeting that he had copied all of the schematics. During the meeting, Awwad provided the undercover FBI agent a thumb drive that contained more schematics of the USS Gerald R. Ford. The undercover FBI agent handed Awwad the "escape plan"—in actuality a manila envelope with no real plan inside—along with $1,000 in currency, shortly before Awwad was arrested.

The schematics of the USS Gerald R. Ford that Awwad provided are information related to the national defense of the United States. The USS Gerald R. Ford, which is currently under construction, is the first in a new class of aircraft carriers. When completed, the USS Gerald R. Ford will be the most advanced aircraft carrier in the world, with approximately 4,000 sailors on board. The schematics contain Naval Nuclear Propulsion Information and they are marked with the handling restriction "NOFORN," which means they are not releasable to foreign persons.

This case was investigated by the FBI's Norfolk Field Office and NCIS Norfolk, in cooperation with the Department of Navy. This case was prosecuted by Assistant U.S. Attorneys Benjamin L. Hatch and Joseph E. DePadilla of the Eastern District of Virginia and Senior Trial Attorney Heather M. Schmidt of the Justice Department's National Security Division.

Case No. 3

Former Connecticut Resident Sentenced to More Than Eight Years in Prison for Attempting to Send U.S. Military Technology to Iran

October 23, 2015

Department of Justice

WASHINGTON—Mozaffar Khazaee, 61, formerly of Manchester, Connecticut, was sentenced today to 97 months in prison and ordered to pay a $50,000 fine by U.S. District Judge Vanessa L. Bryant of the District of Connecticut for violating the Arms Export Control Act by attempting to send to Iran highly sensitive, proprietary, trade secret and export controlled material relating to U.S. military jet engines, which he had stolen from multiple U.S. defense contractors where he had previously been employed.

Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Deirdre M. Daly of the District of Connecticut, Special Agent in Charge Matthew Etre of U.S. Immigration and Customs Enforcement-Homeland Security Investigations (ICE-HSI) Boston, Assistant Director Randall C. Coleman of the FBI's Counterintelligence Division, Special Agent in Charge Craig W. Rupert of the Defense Criminal Investigative Service (DCIS) Northeast Field Office, Special Agent in Charge Danielle Angley of the Air Force Office of Special Investigations and Special Agent in Charge John McKenna of the Department of Commerce's Office of Export Enforcement Boston Office made the announcement.

"Mozaffar Khazaee exploited his privileged access to national security assets to steal highly sensitive military technology with the intent of providing it to Iran," said Assistant Attorney General Carlin. "Violations of the Arms Export Control Act, particularly those involving attempts to transfer sensitive defense technology to a foreign power, are among the most significant national security threats we face, and we will continue to leverage the criminal justice system to prevent, confront, and disrupt them."

"Mozaffar Khazaee betrayed his defense contractor employers and the national security interests of the United States by stealing and attempting to send to Iran voluminous documents containing highly sensitive U.S. defense technology," said U.S. Attorney Daly. "U.S. companies are being relentlessly targeted by those who seek to steal our intellectual property, our trade secrets and our advanced defense technology—whether through a computer hack or cyber intrusion, or through an insider or rogue employee. As this case demonstrates, we will aggressively investigate and hold accountable those who attempt to steal trade secrets and military technology from U.S. industries, whether for their own personal gain or for the benefit of foreign actors."

"Stopping people like Mozaffar Khazaee from providing U.S. military technology to foreign powers is crucial to our national security interests," said Special Agent in Charge Etre. "It's abundantly clear from court records that this individual intended to harm U.S. interests both here and abroad. HSI will continue to work with our federal law enforcement partners to ensure that advanced U.S. military technology is not stolen and illegally exported for the benefit of foreign entities."

"Mr. Khazaee abused a position of trust and responsibility by stealing trade secrets and sensitive information belonging to defense contractors developing some of our most advanced aircraft,"

said Assistant Director Coleman. “His actions could have put our national security at risk. Stopping his plan and holding him accountable for his betrayal was a whole-of-government effort. We will use all available legal means to pursue individuals willing to help our adversaries by stealing our technical know-how.”

“The evidence developed during this investigation and today’s sentencing of Mr. Khazaee illustrate the potential for harm to the U.S. through illegal exportation of sensitive documents and technology,” said Special Agent in Charge Rupert. “DCIS, along with our partner agencies, continues to prioritize and pursue these investigations to curtail any adverse impact to America’s warfighters and shield America’s investment in national defense.”

“This case was enabled by the outstanding teamwork amongst the many federal law enforcement agencies and U.S. Attorney’s office,” said Special Agent in Charge Angley. “Critical was the ability to leverage subject matter experts from the Air Force’s acquisition community who provided the technical assessments of the high value technology. While the conclusion of this case neutralized the threat of this particular person, it also highlights the need for continued and ever more vigilant protection of our critical technologies.”

“Today’s sentencing demonstrates the ongoing cooperation between the U.S. Department of Commerce and other federal law enforcement partners working together in unison to prevent sensitive U.S. origin technology from falling into the wrong hands,” said Special Agent in Charge McKenna.

According to court documents and statements made in court, at different times between 2001 and 2013, Khazaee, a dual citizen of Iran and the United States with a Ph.D. in mechanical engineering, was employed by three separate defense contractors. From at least 2009 through late 2013, Khazaee offered to provide trade secret, proprietary and export controlled defense technology that he had stolen from his U.S. employers to gain employment with state-controlled technical universities in Iran.

Beginning in late 2009, Khazaee corresponded by e-mail with an individual in Iran to whom he attempted to send and in some cases did send documents containing trade secret, proprietary and export controlled material relating to the Joint Strike Fighter (JSF) Program. In one e-mail Khazaee stated that the material he had attached was “very controlled . . . and I am taking [a] big risk.” Khazaee instructed the individual in Iran, “after downloading,” he should “delete everything immediately.”

Analysis of Khazaee’s computer media also revealed cover letters and application documents, dating from 2009 through late 2013, which Khazaee sent to multiple state-controlled technical universities in Iran. In those materials, Khazaee stated that as “lead engineer” in various projects with U.S. defense contractors, he had learned “key technique[s] that could be transferred to our own industry and universities.” Khazaee stated that he wanted to “move to Iran,” that he was “looking for an opportunity to work in Iran,” and that he was interested in “transferring my skill and knowledge to my nation.”

In or about November 2013, while residing in Connecticut, Khazaee attempted to send a large shipping container to Iran. The shipment included, in numerous boxes and on computer media, thousands of highly sensitive technical manuals, specification sheets, test results, technical drawings and data and other proprietary material relating to U.S. military jet engines, including those relating to the U.S. Air Force's F35 JSF program and the F-22 Raptor. The materials in the interdicted shipment had been stolen from U.S. defense contractors where Khazaee had worked and many documents were prominently labeled with strict export control warnings. Khazaee did not apply for nor did he obtain any license to export any of the documents and the export or attempted export of such material to Iran is illegal.

On Jan. 9, 2014, Khazaee was arrested at the Newark Liberty International Airport before boarding a flight to Iran. Search warrants executed on Khazaee's checked and carry-on luggage revealed additional hard copy documents and computer media containing sensitive, proprietary, trade secret and export controlled documents relating to U.S. military jet engines. Khazaee was also found in the possession of $59,945.00 in as-yet undeclared cash, which he had split up into increments of approximately $5,000 and secreted in multiple bank envelopes in various places in his carry-on luggage.

The hard copy and electronic material that Khazaee stole and sought to transfer to Iran totaled some 50,000 pages and was reviewed by experts from both the U.S. Air Force and the victim defense contractors. In addition to the materials relating to the JSF Program and the F-22 Raptor, Khazaee also had documents from numerous other U.S. military engine programs, including the V-22 Osprey, the C130J Hercules and the Global Hawk engine programs. In total, Khazaee sought to export approximately 1,500 documents containing trade secrets and approximately 600 documents containing highly sensitive defense technology.

According to analyses by the U.S. Air Force and victim defense contractors, the technical data that Khazaee stole would have helped Iran "leap forward" ten years or more in academic and military turbine engine research and development, reducing their investment in such technology by one to two billion dollars and potentially enhancing the development and effectiveness of their weapon systems.

Khazaee has been detained since his arrest on Jan. 9, 2014. On Feb. 25, 2015, he pleaded guilty to one count of unlawful export and attempted export of defense articles from the U.S. in violation of the Arms Export Control Act.

This case was investigated by the ICE-HSI' New England Division, the FBI's New Haven Division, the Defense Criminal Investigative Service in New Haven, the U.S. Air Force's Office of Special Investigations in Boston and the Department of Commerce's Office of Export Enforcement in Boston.

Assistant Attorney General Carlin and U.S. Attorney Daly also commended the efforts of the many other agencies and offices that were involved in this investigation, including the U.S. Attorney's Offices of the Central District of California, the Southern District of Indiana and the District of New Jersey; ICE-HSI in Los Angeles; the U.S. Customs and Border Protection Service (CBP) in Los Angeles; the U.S. Air Force's Office of Special Investigations in Los

Angeles; as well as ICE-HSI, CBP and FBI in New Jersey; and HSI, FBI and DCIS in Indianapolis.

This case is being prosecuted by Assistant U.S. Attorney Stephen Reynolds of the District of Connecticut and Trial Attorney Brian Fleming of the Justice Department's Counterintelligence and Export Control Section.

Violations of Standards of Conduct

U.S. States and territories have laws and regulations, including standards of conduct, that cover engineering practice. These standards vary from state to state. For the purposes of the present course, the standards of two states were selected and are given in Appendices A and B. Taken together, these two standards address most of the issues present in the standards of all states.

All of the convicted individuals violated several of the Standards of Conduct of both State A and B. First, they endangered the American public's national security by stealing restricted technology and trade secrets and providing or attempting to provide them to foreign governments. This clearly violates State B Standard (3)(E), which states that "[Engineers'] primary obligation is to protect the safety, health, and welfare of the public."

Second, they violated State A Standard (6)(i), which states that "Use by a professional engineer of his engineering expertise and/or his professional engineering status to commit a felony" constitutes "misconduct in the practice of engineering." The felonies consisted of economic espionage, and violation of the Arms Export Control Act.

Third, they similarly violated State A Standard (6)(r), which states that "Revealing facts, data or information obtained in a professional capacity without the prior consent of the professional engineer's client or employer except as authorized or required by law" constitutes "misconduct in the practice of engineering."

Fourth, they violated State B Standard (3)(C), which states that engineers shall "In the conduct of their practice, not knowingly violate any state or federal criminal law.

Fifth, they violated State B Standard (3)(J), which states that engineers shall "Make full disclosure, suitably documented, to their employers or clients of potential conflicts of interest, or other circumstances which could influence or appear to influence their judgment on significant issues or the unbiased quality of their services," the conflict here of being loyalty to a foreign government while employed by the U.S. government.

Lastly, they violated State A Standard (6)(k), which states that engineers "shall not knowingly associate with … any person or firm which he knows or has reason to believe is in business or professional practices of a fraudulent or dishonest nature," the persons in question being the foreign agents engaged in stealing U.S. technical data.

Appendix A. Standards of Conduct for State A

(1) Pursuant to State statute, the board hereby specifies that the following acts or omissions are grounds for disciplinary proceedings.

(2) A professional engineer shall not advertise in a false, fraudulent, deceptive or misleading manner. As used in State statutes, the term "advertising goods or services in a manner which is fraudulent, false, deceptive, or misleading in form or content" shall include without limitation a false, fraudulent, misleading, or deceptive statement or claim which:

(a) Contains a material misrepresentation of facts;

(b) Omits to state any material fact necessary to make the statement in the light of all circumstances not misleading;

(c) Is intended or is likely to create an unjustified expectation;

(d) States or implies that an engineer is a certified specialist in any area outside of his field of expertise;

(e) Contains a representation or implication that is likely to cause an ordinary prudent person to misunderstand or be deceived or fails to contain reasonable warnings or disclaimers necessary to make a representation or implication not deceptive;

(f) Falsifies or misrepresents the extent of his education, training or experience to any person or to the public at large, tending to establish or imply qualification for selection for engineering employment, advancement, or professional engagement. A professional engineer shall not misrepresent or exaggerate his degree of responsibility in or for the subject matter of prior assignments;

(g) In any brochure or other presentation made to any person or to the public at large, incident to the solicitation of an engineering employment, misrepresents pertinent facts concerning a professional engineer's employer, employees, associates, joint ventures, or his or their past accomplishments with the intent and purpose of enhancing his qualifications and his works.

(3) A professional engineer, corporation or partnership, or other qualified business organization ("firm") shall not practice engineering under an assumed, fictitious or corporate name that is misleading as to the identity, responsibility or status of those practicing thereunder or is otherwise false, fraudulent, misleading or deceptive within the meaning of State Administrative Code. When a qualified business organization or individual is practicing engineering as a sole proprietor under a combination of his own given name, and terms such as "engineering," "and associates" or "and company," then said person or qualified business organization is practicing engineering under a fictitious name, and must be qualified by a State professional engineer.

(4) A professional engineer shall not be negligent in the practice of engineering. The term negligence set forth in State statutes, is herein defined as the failure by a professional engineer to utilize due care in performing in an engineering capacity or failing to have due regard for acceptable standards of engineering principles. Professional engineers shall approve and seal

only those documents that conform to acceptable engineering standards and safeguard the life, health, property and welfare of the public.

Failure to comply with the procedures set forth in the Responsibility Rules as adopted by the board of Professional Engineers shall be considered as non-compliance with this section unless the deviation or departures therefrom are justified by the specific circumstances of the project in question and the sound professional judgment of the professional engineer.

(5) A professional engineer shall not be incompetent to practice engineering. Incompetence in the practice of engineering as set forth in State statutes, shall mean the physical or mental incapacity or inability of a professional engineer to perform the duties normally required of the professional engineer.

(6) A professional engineer shall not commit misconduct in the practice of engineering. Misconduct in the practice of engineering as set forth in State statutes, shall include, but not be limited to:

(a) Expressing an opinion publicly on an engineering subject without being informed as to the facts relating thereto and being competent to form a sound opinion thereupon;

(b) Being untruthful, deceptive, or misleading in any professional report, statement, or testimony whether or not under oath or omitting relevant and pertinent information from such report, statement or testimony when the result of such omission would or reasonably could lead to a fallacious conclusion on the part of the client, employer or the general public;

(c) Performing an engineering assignment when not qualified by training or experience in the practice area involved;

1. All professional engineer asbestos consultants are subject to the provisions of State statutes and administrative law, and shall be disciplined as provided therein.

2. The approval of any professional engineer as a “special inspector” under the provisions of State statute., does not constitute acceptance by the board that any such professional engineer is in fact qualified by training or experience to perform the duties of a “special inspector” by virtue of training or experience. Any such professional engineer must still be qualified by training or experience to perform such duties and failure to be so qualified could result in discipline under this chapter;

(d) Affixing a signature or seal to any engineering plan of document in a subject matter over which a professional engineer lacks competence because of inadequate training or experience;

(e) Offering directly or indirectly any bribe or commission or tendering any gift to obtain selection or preferment for engineering employment with the exception of the payment of the usual commission for securing salaried positions through licensed employment agencies;

(f) Becoming involved in a conflict of interest with an employer or client, without the knowledge and approval of the client or employer, but if unavoidable a professional engineer shall immediately take the following actions:

1. Disclose in writing to his employer or client the full circumstances as to a possible conflict of interest; and,

2. Assure in writing that the conflict will in no manner influence the professional engineer's judgment or the quality of his services to his employer or client; and,

3. Promptly inform his client or employer in writing of any business association, interest or circumstances which may be influencing his judgment or the quality of his services to his client or employer;

(g) Soliciting or accepting financial or other valuable considerations from material or equipment suppliers for specifying their products without the written consent to the engineer's employer or client;

(h) Soliciting or accepting gratuities directly or indirectly from contractors, their agents or other parties dealing with the professional engineer's client or employer in connection with work for which the professional engineer is responsible without the written consent of the engineer's employer or client;

(i) Use by a professional engineer of his engineering expertise and/or his professional engineering status to commit a felony;

(j) Affixing his seal and/or signature to plans, specifications, drawings, or other documents required to be sealed pursuant to State statute, when such document has not been personally prepared by the engineer or prepared under his responsible supervision, direction and control;

(k) A professional engineer shall not knowingly associate with or permit the use of his name or firm name in a business venture by any person or firm which he knows or has reason to believe is engaging in business or professional practices of a fraudulent or dishonest nature;

(l) If his engineering judgment is overruled by an unqualified lay authority with the results that the public health and safety is threatened, failure by a professional engineer to inform his employer, responsible supervision and the responsible public authority of the possible circumstances;

(m) If a professional engineer has knowledge or reason to believe that any person or firm is guilty of violating any of the provisions of State statute, or any of these rules of professional conduct, failure to immediately present this information to the board;

(n) Violation of any law of the State directly regulating the practice of engineering;

(o) Failure on the part of any professional engineer or qualified business organization to obey the terms of a final order imposing discipline upon said professional engineer or qualified business organization;

(p) Making any statement, criticism or argument on engineering matters which is inspired or paid for by interested parties, unless the professional engineer specifically identifies the interested parties on whose behalf he is speaking, and reveals any interest he or the interested parties have in such matters;

(q) Sealing and signing all documents for an entire engineering project, unless each design segment is signed and sealed by the professional engineer in responsible charge of the preparation of that design segment;

(r) Revealing facts, data or information obtained in a professional capacity without the prior consent of the professional engineer's client or employer except as authorized or required by law.

(s) Renewing or reactivating a license without completion of Continuing Education (CE) hours and subject areas as required by State statute and administrative code.

Appendix B. Standards of Conduct for State B

PURPOSE: This rule establishes a professional code of conduct for professional engineers.

(1) Definitions.

(A) Board—The Board for Professional Engineers.

(B) Licensee—Any person licensed as a professional engineer under the provisions of State statutes.

(2) The State Rules of Professional Conduct for Professional Engineers Preamble reads as follows: The board adopts the following rules, referred to as the rules of professional conduct. These rules of professional conduct are binding for every licensee. Each person licensed is required to be familiar with the rules of the board. The rules of professional conduct will be enforced under the powers vested in the board. Any act or practice found to be in violation of these rules of professional conduct may be grounds for a complaint to be filed with the Administrative Hearing Commission.

(3) In practicing professional engineering, a licensee shall—

(A) Act with reasonable care and competence and apply the technical knowledge and skill which are ordinarily applied by professional engineers of good standing, practicing in the State. In the performance of professional services, licensees hold their primary responsibility to the public welfare which should not be compromised by any self-interest of the client or the licensee.

(B) Undertake to perform professional engineering services only when they are qualified by education, training, and experience in the specific technical areas involved.

(C) In the conduct of their practice, not knowingly violate any state or federal criminal law.

(D) Comply with state laws and regulations governing their practice. In the performance of professional engineering services within a municipality or political subdivision that is governed by laws, codes, and ordinances relating to the protection of life, health, property, and welfare of the public, a licensee shall not knowingly violate these laws, codes, and ordinances.

(E) Recognize that their primary obligation is to protect the safety, health, property, or welfare of the public. If the professional judgment is overruled under circumstances where the safety, health, property, or welfare of the public are endangered, they are to notify their employer or client and other authority as may be appropriate.

(F) Not assist non-licensees in the unlawful practice of professional engineering.

(G) Not assist in the application for licensure of a person known by the licensee to be unqualified in respect to education, training, experience, or other relevant factors.

(H) Truthfully and accurately represent to others the extent of their education, training, experience, and professional qualifications and not misrepresent or exaggerate the scope of their responsibility in connection with prior employment or assignments.

(I) Not accept compensation, financial or otherwise, from more than one party, for services pertaining to the same project, unless the circumstances are fully disclosed and agreed to by all interested parties. The disclosure and agreement shall be in writing.

(J) Make full disclosure, suitably documented, to their employers or clients of potential conflicts of interest, or other circumstances which could influence or appear to influence

their judgment on significant issues or the unbiased quality of their services.

(K) Not offer, give, solicit, or receive, either directly or indirectly, any commission, contributions, or valuable gifts, in order to secure employment, gain an unfair advantage over other licensees, or influence the judgment of others in awarding contracts for either public or private projects. This provision is not intended to restrict in any manner the rights of licensees to participate in the political process; to provide reasonable entertainment and hospitality; or to pay a commission, percentage, or brokerage fee to a bona fide employee or bona fide established commercial or marketing agency retained by the licensee.

(L) Not solicit or accept financial or other valuable consideration, either directly or indirectly, from contractors, suppliers, agents, or other parties in return for endorsing, recommending, or specifying their services or products in connection with work for employers or clients.

(M) Not attempt to, directly or indirectly, injure the professional reputation, prospects of practice or employment of other licensees in a malicious or false manner, or both.

(N) Not reveal confidential, proprietary, or privileged facts or data, or any other sensitive information obtained in a professional capacity without the prior consent of the client or employer except as authorized or required by law or rules of this board.

(4) Licensees having knowledge of any alleged violation of this Code shall cooperate with the proper authorities in furnishing information or assistance as may be required.