DISCUSS THE UNIQUE CYBERSECURITY ISSUES AS APPLICABLE TO THE FOLLOWING CRITICAL INFRASTRUCTURES. SPECIFICALLY DISCUSS THE RESPECTIVE POTENTIAL VULNERABILITIES, RISKS, AND CONCERNS, CURRENT GOVERNMENT/INDUSTRY ACTIVITIES, AND PRESENT YOUR RECOMMENDATIONS REGARDING ENHANCED CYBERSECURITY OF THESE KEY NATIONAL ASSETS . . .

[#2] ...REGARDING THE PETROCHEMICAL CRITICAL INFRASTRUCTURE:

THE PETROCHEMICAL (“BIG OIL”) INDUSTRY FACES UNIQUE CHALLENGES OF SAFETY IN THEIR DAILY OPERATIONS IN DEALING WITH A WIDE VARIETY OF HAZARDOUS CHEMICALS ON A DAILY BASIS. VULNERABILITIES INCLUDE EXPOSURE TO THESE MATERIALS, SABOTAGE IN THE EVENT OF A STUXNET-LIKE CYBERATTACK, AND A GEOPOLITICAL AND ECONOMIC INFLUENCE REGARDING PRICE FLUCTUATIONS, WHICH AFFECT THE MARKETPLACE. RECOMMENDATIONS IN ORDER TO REDUCE THESE VULNERABILITIES INCLUDE THE INCREASED USAGE OF RENEWABLE RESOURCES SUCH AS SOLAR, WIND, GEOTHERMAL AND OCEAN CURRENTS IN ORDER TO ENSURE A STEADY ECONOMIC HORIZON AND REDUCE RISK OF GEOPOLITICAL CONFLICT IN OUR CORNER OF THE WORLD.

[#3] ...REGARDING THE FINANCIAL CRITICAL INFRASTRUCTURE:

WALL STREET AND THE BANKING SECTOR FACE STIFF INTERNATIONAL COMPETITION, REGULATION AND GOVERNMENT OVERSIGHT, BUT CORRUPTION REMAINS, MAINLY DUE TO THE HUMAN FACTOR. THE KINETICS OF AN ATTACK UPON THE FINANCIAL SECTOR IS MINIMAL, BUT AS 9/11 CLEARLY DEMONSTRATED, THE SYMBOLOGY OF HITTING A FINANCIAL CENTER WITH A KINETIC WEAPON CAN BE UNFORGETTABLE. LESS OBVIOUS VULNERABILITIES INCLUDE DAILY WEB-BASED AND RETAIL-BASED TRANSACTIONS INVOLVING CONSUMER DATA, ESPECIALLY SINCE 2013. AS WE KNOW, GOVERNMENT INVESTIGATIONS HAVE ALREADY YIELDED A CYBERNETIC AND PAPER TRAIL OF CRIMINAL ACTIVITY RELATED TO THE FUNDING OF INTERNATIONAL TERRORIST ACTIVITIES INCLUDING ISIS. MY STRONGEST RECOMMENDATIONS WOULD INCLUDE A STRONGER MATHEMATICAL ENCRYPTION MODEL THAT WOULD PRESERVE THE INTEGRITY AND SAFETY OF EACH AND EVERY TRANSACTION, WHILE USING BEST FORENSIC PRACTICES TO ELIMINATE THREATS OF MONEY LAUNDERING AND RELATED CYBER CRIMES OF ALL SCOPES, LARGE AND SMALL.

[#4] ...REGARDING THE TRANSPORTATION CRITICAL INFRASTRUCTURE:

ROADS, RAILROADS, BRIDGES, TUNNELS, AIRPORTS, SEAPORTS AND ALL OTHER MANNER OF PHYSICAL TRANSPORTATION ALL FACE A SIMILAR DANGER OF INTEGRITY NOT UNLIKE A PIPELINE OR DATA NETWORK LINE OR NODE. THE PUBLIC EXPECTATION THAT THE VEHICLES INVOLVED ARE ABLE TO WITHSTAND A REASONABLE LEVEL OF EXTERNAL INTERFERENCE FROM SUCH SOURCES AS SEVERE WEATHER, NATURAL TOPOLOGY/GEOLOGY, AND RECONSTRUCTION OF THE INFRASTRUCTURE DUE TO NATURAL WEAR AND TEAR OVER TIME. VULNERABILITIES INCLUDE BOTTLENECKS CAUSED BY CONSTRUCTION OR RUSH HOUR TRAFFIC WHICH WOULD CAUSE A LARGE VOLUME OF VEHICLES TO ACCUMULATE WITHIN MINUTES, PERFECT FOR A TIMED ATTACK. MOST NOTABLE IS A RECENT DEMONSTRATION OF A VEHICLE ON A HIGHWAY, ATTACKED WITH A BARRAGE OF ELECTRONIC SIGNALS WHICH

INTERACTED WITH A CENTRAL SCADA SYSTEM, EVENTUALLY DISABLING THE VEHICLE ON I-70 HERE IN NORTH COUNTY OF ST. LOUIS. POINT BEING, WE ARE MOST SUBJECT TO ATTACK WHEN NODES CLUSTER, SUCH AS IN A TRAFFIC SYSTEM IN A MAJOR CITY. THEREFORE MY RECOMMENDATIONS BEGIN WITH A STRONGER ONION-LIKE MULTILAYERED PROTECTION MODEL IN MAJOR HUBS AND DESTINATIONS, WHILE NOT NEGLECTING THE ABSENCE OF PROTECTIONS IN RURAL AREAS IN ORDER TO SIMPLY GAIN ACCESS TO MAJOR CENTERS. AS STATED, THESE PROTECTIONS WOULD INCLUDE A MULTILAYERED APPROACH OF DETECTION TOOLS IN ORDER TO REDUCE THE THREAT OF EXPLOSIVE DEVICES, OR OTHER HARDWARE, (TIMED, COMPUTATIONAL OR OTHERWISE), THAT WOULD ENDANGER THE PUBLIC SAFETY DURING A TIME OF HIGH TRAVEL VOLUME, SUCH AS THE END-OF-YEAR HOLIDAYS.

[#5] FINALLY, PROVIDE YOUR OVERALL ASSESSMENT OF CYBERSECURITY AS APPLIED TO CRITICAL INFRASTRUCTURE, THE ACTORS, THE CURRENT STATE OF AMERICA'S SECURITY, THE COURSE PRIVATE INDUSTRY IS TAKING TO PROTECT THEIR ASSETS, THE GOVERNMENT'S EFFORTS TO MANAGE THE THREAT, AND HOW YOU VIEW THE OVERALL RISKS TO THE NATION FROM THIS THREAT. BE BOLD AND INNOVATIVE.

I VIEW RICHARD CLARKE'S DISCUSSION TO BE ENGAGING, INSIGHTFUL, ESPECIALLY AUTHORITATIVE, AND A TRUE WAKE UP CALL TO THE DANGERS FACING THE INTERNATIONAL COMMUNITY. I WORRY THAT A MINORITY OF PUBLIC CITIZENS HAVE BECOME JADED TO SUCH ALARM BELLS, WHICH MAKES OUR JOBS OF LEARNED CYBERSECURITY EVANGELICALS EVEN MORE OF A NOBLE CHALLENGE. I ALSO GREATLY APPRECIATE THE WEEKLY IN-CLASS DISCUSSIONS WHICH COMPLEMENT THESE TEXTS. BECAUSE OF THE GREAT STRENGTHS IN OUR OFFENSIVE CAPABILITIES IN OUR MILITARY AND INTELLIGENCE COMMUNITIES, I FEAR NOT THE CAPABILITIES OF OFFENSIVE RETALIATION, WHEN THIS NATION WILL EVENTUALLY SUFFER A GREAT CYBERATTACK, BUT RATHER THE TECHNICAL UNDERSTANDING OF OUR ELECTED POLITICIANS AND THE GREATER MATURITY OF OUR GOVERNMENT WHEN NOT PASSING LAWS THAT EXPERTS CONTINUALLY TESTIFY WOULD MINIMIZE OUR EXPOSURES. I WOULD FURTHER EXPECT PRIVATE INDUSTRY TO TAKE EVERY REASONABLE STEP IN ORDER TO PROTECT THEIR OWN INTERESTS FOR FEAR OF EXPOSURE TO LIABILITY AND CRIMINAL DAMAGE REGARDING THEIR BOTTOM LINES, BUT I HAVE FAITH THAT EVENTUALLY WE WILL STEP FORWARD IN THE RIGHT DIRECTION BEFORE IT IS TOO LATE TO DO SO.