**MINUTES OF MEETING**

Committee Title: Information Systems Technical Advisory Committee (ISTAC)

Date: July 24-25, 2019

Time: July 24 from 9:10 AM to 4:00 PM (open session)

 July 25 from 9:01 AM to 12:28 PM (closed session)

Location: July 24 at Qualcomm, Bldg QRC, San Diego, CA

 July 25 at Qualcomm, Bldg QRC, San Diego, CA

**Agenda Item Presentations/Discussions:**

**PUBLIC/OPEN SESSION (July 24, 2019)**

The meeting opened at 9:10 AM. Approximately 27 people were in attendance.

Opening and Announcements: Jonathan Wise of Keysight Technologies, Inc. (and ISTAC chair) opened the meeting by thanking Qualcomm for hosting, and Kathleen Gebeau of Qualcomm made some welcoming and procedural comments. Jonathan continued with introductions and request for comments from the public. There were no public comments.

-Mark Renfeld of Hewlett-Packard Enterprise (and ISTAC co-chair) made a brief presentation noting that Wikipedia incorrectly describes Adjusted Peak Performance (APP) as having been replaced with Gigaflops (GFLOPS) and noting that 2019 marks the 40th anniversary of the Export Administration Act of 1979.

-Wassenaar proposals for 2020 are due to BIS on or about November 1, 2019, and by that date should be fully developed (not draft) and if appropriate should be reviewed/vetted with BIS beforehand.

Meeting Dates: The next meeting dates are:

* Wed-Thurs, Nov 6-7, 2019 (Wash DC/BIS/HCHB)

Elections for Chair: ISTAC DFO Anita Zinzuvadia conducted elections for chairperson(s). A motion to nominate Jonathan Wise and Mark Renfeld was offered and seconded; Jonathan and Mark were unanimously elected as co-chairs.

Working Group Reports: Key points from the Working Group reports were:

Cat 3A (reported by Jonathan Wise): This group has been working on ideas for proposals for the 2020 Wassenaar cycle; details will be presented as a separate agenda item in open session today.

Cat 3B (reported by Steve Lita): There has been no activity in this group since the last meeting.

Cat 4 (reported by Mark Renfeld): This group has been working on an issue raised by Bill Root at the May 2019 meeting, pertaining to the scope of TSR eligibility in ECCN 4E001; details will be presented as a separate agenda item in open session today

Cat 5p1 (reported by Jonathan Wise on behalf of David Lindsay): There has been no activity in this group since the last meeting.

Cat 5p2 (reported by Roz Thomsen): This group has been responding to BIS on questions pertaining to 2019 Wassenaar proposals in Cat 5p2; the most interesting topic is Cryptanalysis as a Service (“CaaS”). Roz also reported that within the EU, the Council of Ministers has proposed a new general license EU008 (for cryptographic items) that has some similarities to US License Exception ENC (but it more restrictive than ENC); the new EU008 appears to seek to harmonize existing UK and German general licenses for cryptographic items

Cybertool (reported by Mark Renfeld): Leadership of this group has been transferred from Mark Renfeld to Tas Giakoumikis; however, Tas was not present at the meeting and there was no update. Roz Thomsen commented that momentum within the EU towards controls on cybertools for reasons related to human rights seems to be lessening; Mike Maney of Veritas Technologies (and ISTAC member) elaborated that one of the main proponents of controls on cybertools was not re-elected to the EU Parliament.

Industry Ideas for 2020 Wassenaar Proposals: Jonathan Wise presented an overview of ideas for possible Cat 3/4/5 Wassenaar proposals for 2020.

The discussion began with proposals that are new/out-of-box since last year:

-3A1b3: This proposal seeks to add a Note (or Technical Note) to the 3A1b3 controls on microwave transistors, to clarify what it a transistor that is within scope of 3A1b3 and what should be evaluated against 3A1b2 or 3A1b4. Notionally, the proposed Note would be:

*Note 3 Input-matched and impedance-matched transistors are not discrete transistors, [as][because] they contain other circuit elements. If these other circuit elements are integrated monolithically with the transistor, then the device is evaluated for control by 3.A.1.b.2, otherwise it is evaluated for control by 3.A.1.b.4.*

Doug Carlson of M/A-Com (and ISTAC member) will take the lead to write this proposal.

-3A2c1: This proposal would modify the control to replace Resolution BandWidth (RBW) with another yet-to-be-determined parameter. RBW exists in the controls for signal analyzers because it was thought to be the inverse of pulse modulation width for signal generators (entry 3A2d1). However, from a technical standpoint industry questions whether the control on RBW adequately achieves the desired national security goal. Identification of an alternate control parameter will require more study and will be coordinated in the Cat 3A Working Group.

-3A2d3 (and 3A2d5): This proposal would widen the bandwidth for signal generators (currently 2.2 GHz) to 8 GHz or 9 GHz within the frequency bands used for 802.11ay (wireless LAN, 56-69 GHz) and automotive anti-collision radar (76-81 GHz). This proposal will be coordinated through the Cat 3A working group.

-3A2h: This proposal would offer editorial rearrangement of the entry for improved clarity; no change in scope of control is contemplated. The issue is that currently 3A2h requires a combination of both 3A2h1 and 3A2h2 such that the only valid ECCN is 3A2h (no subparagraph), the result of which is that critical information on bit-resolution is hidden. The goal is to offer editorial rearrangement to provide for valid subparagraphs for each range of bit resolution. Jonathan Wise will take the lead to write this proposal.

-3A2h: This second proposal would offer another editorial change to introduce the term “digitizer” or “digitization” into the header paragraph and thereby more explicitly articulate what this entry seeks to control. Currently the concept of digitization appears not in the 3A2h header but rather within subparagraph 3A2h1. Jonathan Wise will take the lead to write this proposal.

-3A2 Modular Instruments: This is a notional proposal to investigate the emergence of modular instruments in the 3A2 space where previously there were one-box instruments. The 3A2 controls are written largely as combinations for frequency range and some other parameter: this is appropriate for one-box instruments but is not necessarily appropriate for modular instrument because they intentionally separate functions into separate modules. Development of this proposal will require more study and will be coordinated in the Cat 3A Working Group.

-3B2: This proposal would add a new subparagraph within 3B2 to control test equipment specially designed for testing items specified by 3A1b12. The rationale is that 3A1b12 itself was created quite recently to recognize an important class of items (T/R modules). Entry 3B2 currently controls test equipment specially designed for testing items specified by 3A1b2 or 3A1b3, and it may be a logical extension to include 3A1b12. Brian Baker commented that he is unaware of any T/R modules that are general-purpose, and that it is likely that all T/R modules are in fact specially designed for some purpose/application; this could result in consideration of revision to 3A1b12. Development of this proposal will be coordinated in the Cat 3A Working Group.

-3A225: This proposal is in infancy; it would seek clarification or scope change to 3A225 (Nuclear Supplier’s Group entry) to address the possibility that some frequency changes controlled by 3A225 might be pertinent for testing of electric automobiles. Development of this proposal will require more study and will be coordinated in the Cat 3A Working Group.

The discussion continued with proposals that carried over from last year:

-3A1a7: This proposal would seek an incremental relaxation of the control thresholds for FPGA devices to reflect technology development since the thresholds were last updated in 2014.

-3A1a11: This entry appears to be intended to capture digital processing ICs, but vague control text in a11b may capture divide-by digital devices. This proposal would seek to clarify that 3A1a11 applies only to devices that process data, not any simple digital device simply because it operates above 1.2 GHz (toggle frequency). Trinh Van mentioned that in addition to devices based on compound-semiconductor wafer, there are also devices based on silicon wafer that have thick layers of compound semiconductor such that they may function as if the wafer were compound semiconductor. Hector Rivera suggested that there might be an analogy to entry 3A1a3 (microprocessors based on compound semiconductor); Trinh agreed that this might be an important analogy. Dave Robertson opined that 3A1a11 might be for control of devices used for frequency synthesis. Brian Baker thought that a definition might be needed to clarify what is a semiconductor IC.

-3A1b2: The frequency point of 37 GHz is used in commercial practice to define the operating range of MMICs in the 3A001.b.2.e paragraph (37-43.5 GHz), but the 37 GHz point is part of the 3A001.b.2.d paragraph. Because the 3A001.b.2.d paragraph has power threshold of -70 dBm, it unintentionally captures devices that are designed and intended to operate in the next higher frequency band. To resolve this, it is proposed to change the 3A001.b.2.d paragraph from its current langue “up to and including 37 GHz” to “up to but not including 37 GHz”. In fact, this proposal has not gained traction in the past two years, and therefore it is likely that it might be postponed at least until next year before revisiting it.

-3A1e1b: This proposal would seek further relaxation to the control threshold for energy density for secondary cells, because new chemistries under development are enabling higher energy densities. Specifically, this proposal might seek to relax the current threshold of 350 W-h/kg to at least 400-425 W-h/kg, based on commercial availability of lithium metal cells having energy density of 450 W-h/kg (Hermes family from Solid Energy Systems, [www.solidenergysystems.com](http://www.solidenergysystems.com)). Rama Dasari of Apple, Inc (and ISTAC member) will take the lead to work with the Rechargeable Battery Association (PRBA) to develop this proposal.

-4A3/4D1/4E1: This proposal would seek incremental relaxation of the control thresholds for APP, to recognize technology development of computers (Moore’s Law). Mark Renfeld will take the lead to write this proposal.

-4A3g: This proposal would seek clarification of the definition of “external interconnection” so that the scope of control is clearer, and exporters would more easily understand what it an what is not within scope of this entry. Mark Renfeld will review this and will consider whether to write a proposal.

-Cat 4 Sensitive List: Entries 4D1/4E1 no longer meet the criteria for inclusion in the Sensitive List: There is increasing foreign availability of software and technology comparable to that of WA member states; hardware was already dropped from SL more than a decade ago; and it is illogical that digital computer software and technology on the same list with scramjet engines (9A11), towed acoustic hydrophone arrays (6A1), and plutonium (1C12). Mark Renfeld will review this and will consider whether to write a proposal.

Roz Thomsen of Thomsen & Burke (and ISTAC member) asked whether there would be a proposal on 3E2. David Lindsay (by phone) commented that the next generation Intel Atom processor will be 3E2, and that the Atom processor family is quite old. The ISTAC has for several years consistently proposed deletion of 3E2 and will defer to BIS on whether to develop a proposal for 3E2.

-Action: The several Working Groups will continue to review their respective proposals, with intent to submit well-researched proposals to BIS on or about November 1, 2019.

Old Business/Open Business: A review of old/open business was scheduled, but was deferred to the next meeting in November because today’s meeting was running long.

4E001 eligibility for TSR: Mark Renfeld discussed 4E001 eligibility for License Exception TSR; this is an issue that Bill Root raised at the May 2019 ISTAC meeting. The issue is that portions of 4E001 are eligible for TSR, including some 4E001 that is controlled for MT, and technology controlled for MT is traditionally not eligible for TSR. Graphically, this is:



Key points were:

-A model for a solution is 3E001, which states “TSR: Yes, except N/A for MT…” and thus it *seems* that 4E001 should read likewise.

-However, the issue is more complex and nuanced, because 4E001 not only sweeps in MT and releases it under TSR but also does this for 600-series and possibly for ITAR. Moreover, 4E992 gets some MT from 4A101 vis 4D994 and releases it as AT.

-Issues to address are:

1. 4D001 (MT portion): Should it include software for 4A001? If so, should it release through TSR?
2. 4D994 (MT portion): Should it include software for 4A101? If so, should it have AT controls? Severing this link also severs the 4A101-4D994-4E992 link.
3. 4E001 (MT portion): Should it capture technology for 4A001, 4A101, 4A102 (ITAR) and 4A611? If so, should it release through TSR?

Action: Mark will explore this in more detail at the next ISTAC meeting.

Industry Perspective on Export Legislation/Regulation: Steve Lita of ASML US Inc. (and ISTAC member) provided an overview of export-control legislative and regulatory activities from the perspective of industry and industry groups. Key points were:

-Huawei and 68 of its affiliates were added to the Entity List in mid-May because “there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States.”

-A Temporary General License, which expires mid-August, was issued to allow exports to Huawei in some very limited circumstances:

* to maintain and support existing and currently fully operational networks and existing Huawei handsets;
* providing ongoing security research critical to maintaining networks, equipment and handsets; and
* engagement as necessary for the development of 5G standards.

-Industry met with senior U.S. government officials and explained the impact of the Huawei action to U.S. companies, which led to the president’s statements at the G20: “U.S. companies can sell their equipment to Huawei. I’m talking about equipment where there is no great national emergency problem with it. But the U.S. companies can sell their equipment. So we have a lot of the great companies in Silicon Valley and based in different parts of the country, that make extremely complex equipment. We’re letting them sell to Huawei.”

-Although the administration’s policy and practice towards Huawei may have changed, nothing has changed legally. BIS officials are advising companies to submit license applications for items that do not implicate U.S. national security; companies should include in their application information on, for example:

* items’ nexus with defense/national security
* foreign availability
* end-uses for the items
* impact on the U.S. company if it cannot export the items

-At the BIS Update Conference, Secretary Ross stated “[T]o implement the President’s G-20 Summit directive two weeks ago, Commerce will issue licenses where there is no threat to U.S. national security. Within those confines, we will try to make sure that we don’t just transfer revenue from the U.S. to foreign firms”

-In mid-May, the president signed an Executive Order (EO), that directs Commerce to create a new transaction-based regime for the control of information and communications technology (ICT) or services. Once implemented in mid-October, the new regime will authorize Commerce to block any transaction – including imports – that involves ICT or services provided by a foreign adversary, where the transaction poses:

* an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICT or services in the United States;
* an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or
* an unacceptable risk to the national security of the United States or the security and safety of United States persons.

Although the EO does not identify which countries or entities would be considered a foreign adversary, the release of the EO coincided with Huawei’s addition to the Entity List

-The NDAA has passed both the House and Senate and will go to a conference committee.

-There is legislative activity regarding Huawei:

* *Politico* reported that a handful of senators are introducing a bipartisan bill that would clamp down on U.S. companies from doing business with Huawei
* Various bills are attempting to prevent the administration from unilaterally allowing business with Huawei and include congressional approval for the Commerce Department to remove Huawei from the Entity List
* There is a bill that would codify the Executive Order and allow Congress to disapprove any waivers/licenses granted to companies selling parts to Huawei

-Activity continues on emerging and foundational technologies. The Advance Notice of Proposed Rulemaking (ANPR) for emerging technologies was published in November 2018; the ISTAC has already seen the proposal for quantum computing already; and at the BIS Update Conference there was discussion that covered artificial intelligence, robotics and additive manufacturing/3D printing. It is expected that the foundational technologies ANPR will be published in the “next few weeks” and it is quite likely that some 3E991 technologies will be on the list.

-The recently-published BIS regulatory agenda includes three pertinent items:

* RIN 0694-AH84 “Elimination of License Exception Civil End Users (CIV)”
* RIN 0694-AH53 “Expansion of Export, Reexport, and Transfer (In-Country) Controls for Military End Use or Military End Users in the People’s Republic of China (China), Russia, or Venezuela”
* RIN 0694-AH65 “Modification of License Exception Additional Permissive Reexports (APR)”

Kathleen Gebeau asked whether there was any information on the schedule/timing for elimination of CIV; Steve responded that elimination of CIV had been mentioned at BIS Update but that no guidance had been given on the schedule/timing.

-Export controls are being used as international negotiating tools: Japan has imposed restrictions on certain high-tech exports to South Korea, specifically fluorinated polyimide (used in smartphone displays) and resist and high-purity hydrogen fluoride (HF), used during semiconductor manufacturing. Japan will stop preferential treatment for these three materials to Korea; exporters will need to apply for an export license each time they want to ship to Korea, which takes about 90 days. This was initially reported to be a result of a diplomatic dispute concerning a Korean court ruling that ordered Japanese companies to compensate Koreans forced to work under harsh conditions during World War II. However, the Japanese government now says the export restrictions are the result of a review of trade policy and claims there are "weaknesses" in Korea's export control system; certain sensitive items have been exported to Korea with inadequate management by companies (end users).

-Action: This presentation was informational in nature and no specific actions were proposed or required.

ECCN 5B001.b.2.d: Shane Hazzard of Tektronix raised some questions about ECCN 5B001.b.2.d. There is a concern that deletion by Wassenaar in Dec 2016 of paragraphs 5B001.b.2.b and 5B001.b.2.c and the related Technical Note “*For the purpose of 5B001.b.2.c, these techniques include optical heterodyne, homodyne or intradyne techniques*” may result in 5B001.2.d having ambiguous scope. Key points were:

-Analog Coherent Optical (“ACO”) modules with >2.5 GHz bandwidth are COTS items and are used in telecommunications infrastructure and in digital telecommunications equipment. It is unclear whether an ACO itself would be controlled by 5B001.b.2.d. Previously, these would have been controlled by 5B001.b.2.c but they were released by the Technical Note. However, removal of 5B001.b.2.c and the Technical Note resulted in loss of context.

-Rama Dasari asked whether the now-deleted Technical Note could have applied to the entire paragraph 5B001.b.2; Shane was unsure.

-Jonathan Wise wondered whether 5B001.b.2.d could be considered for deletion, and will review the discussions circa 2016 leading to the proposal for deletion of 5A001.b.2.b and 5B001.b.2.c.

-Dave Robertson mentioned RF-over-fiber but was uncertain whether it would be controlled under 5B001.b.2.d; he will study that.

Action: Jonathan Wise will coordinate review of this entry.

Vulnerability Disclosures under Chinese Law: Katie Moussouris of Luta Security spoke on a new Chinese law governing vulnerability disclosures. Key points were:

-This discussion refers to a Chinese law that is described here: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-rules-managing-cybersecurity-vulnerabilities-published-draft-form/>

-This law is promulgated by the Chinese Ministry of Industry and Information Technology.

-Article 3 of the Law captures operators in China and the timeline for disclosures goes beyond (is shorter than) industry standards. This raises an important question of what will happen when/if timelines are broken (not adhered to)?

-Roz Thomsen asked whether Google, which has no presence in China, would have an obligation under this law. Katie thought that Google would have an obligation because, for example, they could have a vulnerability that affects the Android O/S, and thus affects Huawei (because Huawei uses Android).

-Dave Robertson observed that China is moving ahead unburdened by democratic processes, in a manner somewhat aligned to the EU, and wondered whether China is a prime mover in this field? Katie responded that there is movement in the US towards this kind of mandate, and that this could cause risk of unwillingness to disclose vulnerabilities because of an inability to comply with the timelines.

-David Kapan (by phone) noted that the Chinese law seems to be focused primarily on network operators. Katie agreed and noted that Article 3.1 of the regulation seems to distinguish “network product” (hardware) from “network service” (service).

-Katie continued by noting that Articles 8 and 9 mention “administrative punishments” and that enforcement pertains to “causing harm” but that “harm” is undefined. One wonders whether “harm” refers to human health and safety, or to financial/economic activity; or to national security; or to other things; or to some combination of these. Article 10 requires prompt upload of vulnerability details to a database; this seems to be analogous to the US National Vulnerability DataBase (NVDB).

-The comment period for the regulation ended on July 18, 2019. The impact of enforcement remains unclear.

-Dave Robertson asked whether ISO has any proposals for a single cybersecurity body such that notification to that one body would meet all notification requirements, worldwide. Katie was unsure but thought that such a single body could be problematic.

-Roz Thomsen asked if there is a model for vulnerability disclosure that ISO has considered. Katie explained that a “vendor” in the ISO context is the party who is responsible for fixing a vulnerability, although there could be exceptions to this if the vendor is no longer in business.

-Katie continued by noting that notification (of vulnerabilities) to affected parties as quickly as possible is desirable, and that it is customary for there to be an embargo on public release of information while the remedy for the vulnerability is reviewed within a group of trusted vendors and the patches are tested. If there are multiple governments involved, one of them could choose to release the details nationwide, and that would compromise the goal of minimizing information release until the patch is ready. Katie added that when embargoing a vulnerability disclosure, sometimes it is not possible to know who is affected (e.g., if the vulnerability is in a shared library, it might be technically infeasible to identify all affected parties).

-Anita Zinzuvadi commented that for export control a technical note releases from control all vulnerability disclosures. Katie agreed that the consequence of the technical note is that vulnerability disclosers would not be captured by export control but added that it would still be possible to be affected by other regulations and that there could be issues on incident response (although incident response is also be released from export control).

-Hector Rivera asked whether any Chinese companies have expressed a position on this regulation. Katie responded that she is unaware of any feedback/comments on this and that opinions on regulations is the type of information that Chinese companies would be unlikely to share. In short: we don’t know how Chinese companies have reacted to this.

-Steve Lita commented that this regulation would presumably not apply to products created by the Chinese government. Katie agreed and noted that the regulatory requirements could be imposed on anyone else operating in China.

-Action: This presentation was informational in nature and no specific actions were proposed or required.

Order-of-Review for ECCNs 9A515 and 3A611: Hector Rivera of Teledyne (and ISTAC member) raised some questions about the order-of-review for ECCNs 9A515 and 3A611. Key points were:

-The order-of-review for the CCL starts with Category 0, then Category 1, then Category 2 and continues to Category 9.

-Certain rad-hard integrated circuits are controlled in 3A001.a.1 and 3A611. If one has a rad-hard IC that is not controlled in either of those ECCNs, there is a risk that one might conclude that it is EAR99 and overlook the possibility that it could be 9A515. (Although it is likely that if an IC is not 3A001.a.1 it would still be 3A611.)

-ECCN 9A515 is controlled for RS2 whereas 3A611 is controlled for NS1 and RS1. That is, 9A515 is less restrictive than 3A611.

-Brian Baker explained that EAR part 774 Supplement 4 describes the order of review and clarifies to look first at 500/600-series ECCNs before stepping through the Categories in numerical order. Brian also noted that 9A515.e is “specially designed for USML Category XV” and that this is the key to understanding the scope of 9A515: If not 9A515 then go to 600-series or ITAR, else review the CCL categories in numerical order. In summary, start by understanding what is specially designed.

-Hector noted that 3A611.f refers ahead to 3A611.x/3A611.y and that 3A611.y.14 controls certain ASICs.

Action: No specific actions were needed. Interested and affected parties should review 774 Supplement 4.

Implants: Dave Aitel of Immunity (and ISTAC member) and Ryan Speers of River Loop Security (and ISTAC member) spoke about the definitions and history of “Implants”. They covered the history of software implants for both offensive and defensive purposes, including several key traits. These traits included the small footprint, the typical desire for ’stealth’, and other attributes. On the hardware side, a number of attack types that have been publicly discussed were explained and the overlap between those techniques and “legitimate” hardware technologies were discussed. This included overlap between hardware implants and TSV/WLCSP technologies. Those interested in further reading were referred to [https://trmm.net/Modchips](https://nam05.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftrmm.net%2FModchips&data=02%7C01%7C%7Cb265a4fc128849da89d508d719305b92%7C63545f2732324d74a44dcdd457063402%7C1%7C0%7C637005567829266343&sdata=0t5%2BXczosMKrlVReEQrJ%2BSKls025ys4GsQl47Jlc%2Bw8%3D&reserved=0) for reference. Questions were answered for attendees around these and related topics.

Key points were:

-It is unwieldly to address implants through export controls because it would effectively be an end use controls, which is more criminal statute space.

-Remote Access Trojans (RAT) are similar to but different than implants; the differences pertain to permanence and covertness; sometimes the difference is vanishingly small.

-Rootkits are filters; they do this by API hooks and Direct Memory Object Modification of the kernel. Important questions are: What does it hook? How does it get execution in a privileged context? What does it filter? How is it configured or managed? Does it survive reboot (>5 years ago it did, today it doesn’t…reboots are rare)?

-Rootkits allow a “good” someone to hide a process from other users so only the “good” someone can kill the process.

-Implants are not part of the manufacturer’s design and are inserted, without knowledge of the manufacturer, for malicious purposes by third parties. They are a key part of cyber-offense.

-Trinh Van asked whether, in the scenario of a hardware implant, is the implant dormant until it is activated. Ryan explained that hardware implants do not exist in a vacuum but rather hardware and software live together in the ecosystem. For example, hardware can insert software, or hardware can soften a system to allow software to enter the system.

-Hardware implants could be a component on a printed-circuit board, and it might not be easy to identify when a component it added as an implant, because there are many legitimate reasons to modify boards.

-Hardware implants could also be created within an integrated circuit, such as through a change in wire bonding.

-Hardware attacks on the PCB itself are difficult because they typically require many changes (University of Michigan study).

-Roz Thomsen asked if the government market is more advanced than the commercial market. Ryan opined that the government market is not more advanced but that it is more customized/bespoke, more thoroughly tested, and has a different focus. In the commercial sector, there is significant financial effort placed on anti-cheat in gaming.

-Dean White suggested that optical comparators should be an effective method to test for and detect hardware implants/modifications. Ryan agreed but noted that the manufacturer would have a golden image against which to compare, but that users/customers who are removed from the manufacturer do not have the golden image and probably also do not have the optical inspection tools. Dean suggested that this points to the value of a trusted foundry; Ryan agreed.

-Katie Moussouris commented that the gaming industry relies heavily on penetration testing and that the critical question from that industry is the susceptibility to cheating. The economics are such that a multi-million-dollar game could be rendered valueless if it is too easily cheated.

-Roz Thomsen asked whether this can be generalized beyond cybertools to other software (e.g., forensics software. Dave responded that it can be generalized.

Random-as-a-Service: Ryan Speers made a lighthearted presentation about the possibility of Random-as-a-Service (i.e., providing random numbers as a service). The underlying technical principle is that good security depends critically on good random number seeds (i.e., truly random, without patterns that could be exploited) and generating random numbers is difficult. Often, random number generation is based on physics (e.g., lava lamps can be used as the physical basis for generating random numbers).

-A key purpose of this presentation was to encouraging listeners to think about where the line for cryptographic export begins and ends in such contexts.

Action: This presentation was informational in nature and no actions were proposed or required.

ISTAC Charter: Paul Ledet of National Instruments (and ISTAC member) asked about the status of the ISTAC Charter. Anita Zinzuvadia explained that the Executive Order to reduce the of TACs has resulted in review of TACs, including actions to justify the existence of statutory TACs. This activity has not caused on changes to the ISTAC Charter, and the current Charter will remain in force until it is edited/revised.

Semiconductor Circuit Technology Trends (ISSCC Forums): Dave Robertson of Analog Devices, Inc. (and ISTAC member) spoke on trends in semiconductors/integrated circuits that he has observed at the International Solid-State Circuits Conference. Key points were:

-ISSCC is the premier IEEE semiconductor circuits conference, held annually in San Francisco. Traditionally, it has a very strong commercial/industry presence, compared to many conferences that may have a more research/academic focus. There is a combination of peer-reviewed papers, tutorials, evening panel sessions, etc. In addition, each year, there are 5 day-long forums on select topics, intended to encourage discussion of state-of-the-art technology. (The material from these forums is not published– allowing authors to submit material for publication to other journals or conferences later). Looking at forum topics and themes can provide an interesting view to what the semiconductor industry sees as the “hot topics” over the past 3 years. Speakers are invited and selected based on industry leadership on the topics, but also with some emphasis on geographic distribution (which thereby provides some interesting insight into “where” the players are).

-Processors for Artificial Intelligence: topics include deep learning; neuromorphic systems; memory-centric computing; energy-efficiency of machine learning. There are many dual-use issues with AI; the civilian and military uses are analogous.

-Low and Very-Low Power for Remote Sensing: topics include wireless transceivers for LAN and WAN; integrated voltage regulators; intelligent systems for IOT; energy-efficient analog design.

-Very-High-Speed Data: topics include high-performance frequency generation for wireless and wireline systems; wireline transceivers for 50 Gb/s and higher; advanced optical communications: devices, circuits, architectures and algorithms.

-5G and Microwave: Circuits and Architectures for Wireless Sensing, Radar and Imaging; Circuit and Systems for mm-wave Multi-Antenna Systems; Sub-6GHz 5G Radio Circuits and Systems.

-Other themes: topics include Pushing the Performance Limits in Data Converters; FinFETs vs. SOI: A Mixed Signal Circuit Designer’s Perspective; Application-Optimized Data Converters; Advanced Driver Assistance Sensing Networks.

- Speakers on these topics were from many institutions, worldwide.

-Technology has a cycle: 1) capability (proof-of-concept; early products that accomplish something new and not previously available); 2) speed (the concept is known and the goal is to implement the technology to produce something that is better/faster than the competition, e.g. higher speed data conversion, higher clock rate microprocessor); 3) Figure of Merit (optimization on a secondary parameter, e.g., reduction of power consumption); 4) commoditization and cost reduction.

-Dave Aitel asked whether the US is being leap-frogged by China in technology development. Dave Robertson responded that China has very large amounts of data and is ahead of the west on natural language recognition, but that the US maintains a lead in hardware.

Action: This presentation was informational in nature and no actions were proposed or required.

5G Update: Durga Malladi, Senior Vice President and General Manager of 4G/5G at Qualcomm, spoke on 5G; this was an update on his presentation from the July 2018 ISTAC meeting, to reflect developments in 5G in the past year. Key points were:

-The 5G platform-to-the-future will include: on-device, intelligence; extreme reliability; multi-gigabit speed; ultra-low latency; scalable to extreme simplicity; virtually unlimited capacity.

-Devices operating at mmwave are still in the early stages and in only limited infrastructure.

-Latency and reliability are showing up in digitization of manufacturing, removing comm wires in factories.

-The trend towards simplicity has some work to go: 5G in phones and laptops has not yet reached the tiniest form factors (e.g. 5G module has not yet reached the point where it can be used in a simple sensor, such as might be needed for a parking meter).

-5G deployments in 2019 are:

* North America: sub-6 GHz and mmwave
* EU: sub-6 GHz, and mmwave in 2H2019
* Australia/SEA: sub-6 GHz
* South Korea: sub-6 GHz and mmwave
* China: sub-6 GHz
* Japan: sub-6 GHz and mmwave

-Currently, only the US has a significant installation of mmwave 5G; Japan has some token launches and will have broader rollout prior to the 2020 Tokyo summer Olympics.

-Global availability on 5G devices moving faster than 4G (noting sub 6GHz and mmwave), US generally ahead.

-The 5G user experience, as compared to 4G, will be: download latency 3x-20x faster; content download (offline access) 3x-10x faster; streaming playback will increase from 4% of playback at maximum bitrate to 95% at maximum bitrate. Economics: 5G is much cheaper per bit, so carriers are motivated to push it; typical cost of service plans is $65/month for 250 GB. There is only limited use for that much data/speed on mobile handsets, so it sill support larger devices such as laptops.

-Antennae: 5G devices will have multiple antennae modules throughout device, this is necessary based on the way difference users hold the devices. It also allows 3D beam steering/switching and leveraging multiple paths and reflections!

Fixed wireless access will continue to be an important use case in the US to provide suburban and rural broadband. Mmwave radios can provide 10 MB/s, and this is important in rural areas.

-There is a policy question of whether the US, as a nation, has overinvested in mmwave. The answer is that it has not overinvested, and that mmwave will be important to support broadband.

-5G indoor service will provide better security than WiFi. A complementary benefit is that as the user moved from indoors to outdoors, he/she remains 5G-connected.

-5G enables mobile cloud: data will not need to reside on the device, and this reduces concerns about theft (if the data is not on the device, the data cannot be lost/compromised if the device is stolen).

-5G can support industrial IoT, e.g., automobile manufacturing. It is very cost-effective to have good communications on a manufacturing line: if defects are detected, they can be fixed immediately rather than allowing them to propagate to the end of the manufacturing line and then returning the defective item into the line for rework. Industrial IoT can include security cameras, head-mounted displays, handheld terminals, industrial robots, sensors.

-5G can support connected vehicles that communicating directly with people and things: V2V (non-line-of-sight, approaching from blind spot), V2N (navigation rerouting), C2I (infrastructure/ traffic lights/cameras), V2V (viz line-of-sight), V2P (pedestrian, bicyclist). The key technical issue for these applications is that there is not enough time for sensor to talk to cloud to talk back; rather, communication must be done directly between vehicle and immediate area target.

-Dave Aitel asked what is the vehicle communication range. Durga explained that V2V range is function of error rate allowed, so at 90% good rate 100m to maybe 1000m. Further away is more the realm of the cloud, where latency is tolerable. There are two possible methods to handle traffic: each node can either pre-calculate all trajectories for all nearby vehicles, or every vehicle talks constantly to every other vehicle: does one want a computing problem or distributed information problem? VRU = vulnerable roadside units!

-Venu Ranganathan asked for a comparison of 5G technology between Huawei and other technology developers. Durga responded that Huawei 5G technology is deployed mostly in China, with some deployments in the EU and one deployment in Korea. Huawei’s focus is sub-6 GHz and it is weak in mmwave; eventually they will have to include mmwave, this might be a three-year plan for them. Huawei mobile handsets have been disappearing from the EU and elsewhere but remain widely available in China.

-Shane Hazzard asked how “computing-at-the-edge” influences the cloud distribution of data centers. Durga explained that centralized clouds are cheap, but latency from radio access network. For low-latency-essential missions, the user must be close to LAN or part of it, and the computing cannot be centralized. Requires a “federation” strategy between what must be local/low-latency and what must be centralized

-Anita Zinzuvadia asked whether Qualcomm has a technology strategy for 5G. Durga responded that the strategy is in technology development and focuses on quality and fundamental technology rather than on the quantity/number of patents.

-Roz Thomsen commented that it is often reported in the press that Huawei is the most active patent filer, and asked whether Durga had thoughts on the quality of Huawei patents. Durga opined that many of Huawei’s patents are not fundamental technologies but rather are bits and pieces or maybe even shots in the dark (speculative). He added that there is no peer review for patents, with the result that anybody can submit a patent for anything (e.g., the four-legged chair is well known, but that does not prevent a patent filing for a five-legged chair).

Action: This presentation was mostly informational in nature and no specific actions were proposed. The ISTAC working groups will continue to monitor developments in 5G and prepare Wassenaar proposals as appropriate.

Working Groups

Working Group Sessions: The meeting broke into Working Group sessions, and today there were two parallel sessions: Cat 3A, and Cat 4/Cat 5p2/Cyber. Each session lasted approximately 15 minutes. Summaries were not presented to the full ISTAC.

The open session was adjourned at 4:00 PM.