ELECTRONIC DISCOVERY STANDARDIZATION

Eric Hibbard[†]

INTRODUCTION

After a somewhat rocky start, the International Organization for Standardization (ISO), in conjunction with the International Electrotechnical Commission (IEC), Joint Technical Committee 1 (JTC 1), Information Technology, Subcommittee 27 (SC 27), and Security Techniques, is developing an E-Discovery standard with potential global implications. This standard, known as *ISO/IEC 27050, Information Technology—Security Techniques—Electronic Discovery*, seeks to harmonize terminology, describe core concepts, offer guidance in several key areas (e.g., E-Discovery governance, processes, readiness), and identify relevant requirements. While ISO/IEC 27050 is not intended to contradict or supersede local jurisdictional laws and regulations, it is likely to have an impact because International Standards play an important role in cross-border issues, and if nothing else, it could help address the "reasonableness" of one's actions.

I. BACKGROUND ON INTERNATIONAL STANDARDS DEVELOPMENT ORGANIZATIONS (SDOS)

ISO is the world's largest developer of voluntary International Standards and it is an independent, non-governmental organization made up of members from the national standards bodies of 162 countries and 3,368 technical bodies.[1] Since its founding in 1947, ISO has published

† Eric Hibbard is the CTO for Security and Privacy at Hitachi Data Systems, where he leads the Hitachi product-oriented security strategy activities with an emphasis on data/storage security. He is also involved with Hitachi's efforts to secure emerging technologies (cloud security, big data, IoT, M2M), social infrastructure, and critical infrastructure. Mr. Hibbard is a senior security professional with 30+ years of experience working for government, academia, and industry. His expertise spans information assurance, privacy, data storage, cloud computing, eDiscovery, and enterprise information and communications technology (ICT). Hibbard serves as the International Representative for the INCITS/CS1 Cyber Security, Co-Chair of the Cloud Security Alliance International Standardization Council, Co-Chair of the ABA E-Discovery & Digital Evidence Committee, Vice-Chair of the ABA Cloud Computing Committee, Chair of the SNIA Security TWG, and the Chair of IEEE Information Assurance Standards Committee. In addition, he serves as the Editor of ISO/IEC 27040 (Storage Security), Co-Editor of ISO/IEC 17788 (Cloud Computing–Vocabulary and Overview), Project Editor of

over 19,500 International Standards covering almost all aspects of technology, business, and manufacturing (e.g., from food safety to computers, and agriculture to healthcare).[2]

Founded in 1906, the IEC is the world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies, collectively known as "electrotechnology."[3] The IEC reports that "[o]ver 10,000 experts from industry, commerce, government, test and research laboratories, academia and consumer groups participate in IEC Standardization work."[4]

ISO and IEC are two of the three global sister organizations (International Telecommunication Union, or ITU, being the third) that develop International Standards for the world.[5] When appropriate, some or all of these standards development organizations cooperate to ensure that International Standards fit together seamlessly and complement each other: "Joint committees [e.g., JTC 1] ensure that International Standards combine all relevant knowledge of experts working in related areas."[6] All ISO/IEC International Standards are fully consensus-based and represent the needs of key stakeholders of every nation participating in ISO/IEC work: "Every member country, no matter how large or small, has one vote and a say in what goes into an [ISO or] IEC International Standard."[7]

II. STANDARDIZING IT SECURITY TECHNIQUES

Within JTC 1, Subcommittee 27 (SC27) has responsibility for the development of standards for the protection of information as well as information and communications technology (ICT).

ISO/IEC 27050 (Electronic Discovery), and Editor of IEEE Std. 1619r (Cryptographic Protection of Data on Block-Oriented Storage Devices). He is also involved with INCITS/T11, IEEE P1619, ISACA, ISSA, Trusted Computing Group, and IEEE-USA CIPC. Mr. Hibbard is a frequent speaker at international events and has materials published in multiple books. Mr. Hibbard currently holds the (ISC)2 CISSP certification as well as the ISSAP, ISSMP, and ISSEP concentration certifications. He also holds the ISACA CISA certification. His educational background includes a B.S. in Computer Science and a Certificate of Proficiency in Data Communications.

1. *About ISO*, INT'L ORG. FOR STANDARDIZATION, http://www.iso.org/iso/home/about.htm (last visited May 15, 2014).

2. *Id.*

3. *About the IEC*, INT'L ELECTROTECHNICAL COMM'N, http://www.iec.ch/about/?ref=menu (last visited May 15, 2014).

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular, information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including, but not limited to, mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation, and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.[8]

Since convening its first plenary session in April 1990, SC27 has published more than 120 standards and currently has in excess of seventy-five active projects.[9] To manage these projects and the ongoing maintenance associated with the published standards, SC27 is organized into the following working groups (WGs)[10]:

- WG 1: Information security management systems (ISMS)
- WG 2: Cryptography and security mechanisms
- WG 3: Security evaluation, testing, and specification
- WG 4: Security controls and services
- WG 5: Identity management and privacy technologies
- SWG-T: Special working group on transversal items.

To complete the picture, the United States is one of the fifty-three participating countries (voting members) along with seventeen observing countries.[11] Within the United States, the American National Standards Institute (ANSI) serves as the formal United States National Body (USNB) to

8. INT'L ORG. FOR STANDARDIZATION/INT'L ELECTROTECHNICAL COMM'N [ISO/IEC], SC 27 BUSINESS PLAN OCTOBER 2013—SEPTEMBER 2014, at 1.2, ISO/IEC JTC 1/SC 27 N12830 (Sept. 30, 2013).

9. *Id.* § 1.3.1.

10. ISO/IEC, JTC 1/SC 27 IT SECURITY TECHNIQUES, http://www.iso.org/iso/iso_technical_committee?commid=45306 (last visited May 15, 2014).

11. *Id.*

SC27.[12] Under ANSI's auspices, the International Committee for Information Technology Standards (INCITS) serves as the U.S. Technical Advisory Group (TAG) to JTC 1, and INCITS Technical Committee Cyber Security (CS1) has been delegated responsibility to interface with SC27.[13] SC27 meets twice a year, typically during spring and fall, at a wide range of international venues. Plenary sessions, where major decisions are made, occur at the spring meetings.[14]

A. *SC27/WG4 Investigative Projects*

Starting in April 2008 at the SC27 meeting in Kyoto, Japan, SC27/WG4 initiated a Study Period[15] on *Evidence Acquisition Procedure for Digital Forensics*,[16] and issued the New Work Item Proposal (NWIP)[17] after the SC27 meeting in Limassol, Cyprus, in October 2008. This project would be the first of what would become a set of "investigative" projects that focus on incidents, investigation, and evidence.[18] As of this writing, these projects include[19]:

- ISO/IEC 27035 (draft), Information Technology—Security Techniques—Information Security Incident Management (multi-part)
- ISO/IEC 27037: 2012-11-01 (1st ed.), Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence
- ISO/IEC 27038: 2014, Information Technology—Security Techniques—Specification for Digital Redaction

---

12. *About ANSI*, AM. NAT'L STANDARDS INST., http://www.ansi.org/about_ansi/overview/overview.aspx?menuid=1 (last visited May 15, 2014).

13. *CS1—Cyber Security*, INCITS, http://www.incits.org/committees/cs1 (last visited May 15, 2014).

14. ISO/IEC, REVISED DRAFT SC 27 STANDING DOCUMENT 5 (SD5): ISO/IECJTC 1/SC 27 MANAGEMENT GUIDELINES, at 4.1, ISO/IEC JTC 1/SC 27 N13525 (Dec. 31, 2013).

15. Within SC27, new potential projects typically go through a vetting process that involves the formation of an ad hoc committee, appointment of a Rapporteur, and then a call for comment and contributions from interested National Bodies. These Study Periods run at least six months and can be extended, assuming there is interest in doing so. The findings of the Study Period can result in a recommendation for no action (i.e., there is insufficient support or expertise within SC27 to pursue a project) or to proceed with one or more projects (i.e., initiation of New Project ballots).

16. ISO/IEC, CALL FOR RAPPORTEUR AND CONTRIBUTIONS TO WG 4 STUDY PERIOD ON EVIDENCE ACQUISITION PROCEDURE FOR DIGITAL FORENSICS, ISO/IEC JTC 1/SC 27 N6428 (Apr. 18, 2008).

17. *Id.*

18. ISO/IEC, DRAFT 3 OF ISO/IEC JTC 1/SC 27/WG 4 SD 3, COORDINATION OF INVESTIGATIVE PROJECTS, at 1, ISO/IEC JTC 1/SC 27/WG 4 N395 (Jan. 30, 2014).

19. ISO/IEC, SYSTEM AND SOFTWARE ENGINEERING—INFORMATION TECHNOLOGY—GOVERNANCE OF DIGITAL FORENSIC RISK FRAMEWORK, ISO/IEC JTC 1/SC40 N30121 (Nov. 13, 2013).

- ISO/IEC 27040 (draft), Information Technology—Security Techniques—Storage Security
- ISO/IEC 27041 (draft), Information Technology—Security Techniques—Guidance on Assuring Suitability and Adequacy of Investigation Methods
- ISO/IEC 27042 (draft), Information Technology—Security Techniques—Guidelines for Analysis and Interpretation of Digital Evidence
- ISO/IEC 27043 (draft), Information Technology—Security Techniques—Incident Investigation Principles and Processes
- ISO/IEC 27050 (draft), Information Technology—Security Techniques—Electronic Discovery (multi-part)

The above investigative projects are not intended to contradict or supersede local jurisdictional laws and regulations, and further, they are expected to have relevance outside of the legal domain.[20]

It is important to note that the USNB has argued on several occasions that the investigative projects were outside the scope of SC27, and further, that SC27 did not have the technical expertise to deal with some of these topics.[21] The USNB concerns were overridden because of the perceived needs in developing countries; in some countries, ISO standards carry the weight of laws or regulations.[22]

B. *Genesis of the ISO/IEC 27050 Electronic Discovery Project*

At about the same time—October 2008—that SC27/WG4 began development of ISO/IEC 27037, the American Bar Association's (ABA) Section of Science & Technology Law (SciTech) formed the E-Discovery and Digital Evidence (EDDE) Committee.[23] At the Committee's first meeting in November 2008 in Washington, D.C., a member of INCITS/CS1 reached out to the EDDE Committee for reaction and comments on the NWIP for ISO/IEC 27037. These initial interactions eventually transitioned into a more formal liaison relationship between INCITS/CS1 and ABA

20. ISO/IEC, REPORT ON THE 13TH MEETING OF ISO/IEC JTC 1/SC 27/WG 4, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—SECURITY CONTROLS AND SERVICES, HELD IN ROME, ITALY, 2012-10-22 to 2012-10-26, § 3.3, ISO/IEC JTC 1/SC 27/WG 4 N 51 (Nov. 21, 2012).

21. There is no single source for this. This is a comment by the USNB International Representative (CS1 officer) who has been involved in these discussions and pressed the U.S. position in SC27 meetings.

22. There is no single source for this. This is a comment by the USNB International Representative (CS1 officer) who has been involved in these discussions and pressed the U.S. position in SC27 meetings.

23. *Section of Science & Technology Law: E-Discovery and Digital Evidence Committee*, ABA, http://apps.americanbar.org/dch/committee.cfm?com=ST203001 (last updated Mar. 4, 2014).

SciTech in February 2009.[24] This relationship continued throughout the development of ISO/IEC 27037 and to this day, as SC27 has expanded its investigative projects. The net result of this liaison relationship is that the ABA SciTech expertise improved the quality of the USNB comments and contributions on SC27's quasi-legal drafts, while at the same time giving the ABA SciTech experts insight into the SC27 projects and the international standardization process.

In December 2011, at the EDDE Committee face-to-face meeting in Washington, D.C., the topic of E-Discovery standardization (both domestic and international) was discussed at length.[25] The general sense of the participants was that there was definite merit in having an international standard, but organizational politics made it unlikely that a domestic project would result in anything useful. That said, the mechanics and feasibility of pursuing such an endeavor were unknown, so the Liaison Officer to INCITS/CS1 was tasked with determining the USNB's level of interest in serving as a project sponsor and outlining the process.

The response from the INCITS/CS1 members was positive, with the caveat that the ABA SciTech would need to provide support if the project was successfully launched in SC27.[26] Given the lengthy lead times often required for SC27 proposals, INCITS/CS1 needed a go/no-go recommendation from the EDDE Committee by March 2012, so that a proposal for a SC27 Study Period could be developed, approved by INCITS/CS1, and then submitted to SC27 as an on-time contribution from the USNB (i.e., routed through INCITS and then ANSI), which would enable consideration of the proposal at the April 2012 SC27 meeting in Stockholm, Sweden.

The EDDE Committee was briefed at its February 2012 face-to-face meeting in San Francisco, California. A defining moment for the E-Discovery standardization occurred at this meeting when the Honorable John M. Facciola (U.S. Magistrate Judge, U.S. District Court, District of Columbia) brought the Committee to a decision point by moving to support the development of a standard; then the Honorable Andrew J. Peck (U.S. Magistrate Judge, U.S. District Court, Southern District of New York)

24. INT'L COMM. FOR INFO. TECH. STANDARDS (INCITS), DRAFT MINUTES OF THE SEVENTEENTH MEETING OF INCITS TECHNICAL COMMITTEE CS1, CYBER SECURITY, § 7.2, CS1-2009-00014-006 (Feb. 12, 2009).

25. *See* INCITS, DRAFT MINUTES—THIRTY-THIRD MEETING OF INCITS TECHNICAL COMMITTEE CS1, CYBER SECURITY, CS1-2012-00058-000 (Mar. 5, 2012).

26. *Id.* at 19.

promptly seconded it.[27] There were no objections and INCITS/CS1 was notified of the decision.[28]

INCITS/CS1 quickly drafted a contribution for the SC27 meeting in Stockholm that outlined the potential need for an E-Discovery standard and proposed a six-month Study Period.[29] In Stockholm, representatives from the United States, Sweden, Great Britain, Japan, Singapore, South Africa, Germany, Canada, Estonia, and INTERPOL participated in the USNB-lead discussion and they agreed that E-Discovery could be a useful addition to the existing series of digital evidence and incident investigation related standards.[30] A new study period on E-Discovery was therefore initiated and a call for contributions[31] was sent out to the NBs. Angus Marshall (United Kingdom) and Eric Hibbard (United States) were appointed the co-Rapporteurs for the six-month study period.[32]

Steven Teppler, Esq., and Eric Hibbard, Co-chairs of the EDDE Committee, took on the challenge of developing a United States contribution for the E-Discovery Study Period.[33] The goal was to provide enough text so that it would be relatively easy to construct a New Work Item Proposal (NWIP) from the contribution and the Study Period terms of reference. This contribution leveraged the Seventh Circuit Electronic Discovery Pilot Program Principles[34] and the New York Bar Association's *Best Practices in E-Discovery in New York State and Federal Courts*.[35]

The E-Discovery Study Period was concluded at the SC27 meeting in Rome, Italy, in October 2012.[36] Both the United States and United Kingdom

---

27. INCITS, DRAFT MINUTES FOR THE THIRTY-FOURTH MEETING OF INCITS TECHNICAL COMMITTEE CS1, CYBER SECURITY, at 40, CS1-2012-00038-004 (Mar. 21–22, 2012).

28. *Id.*

29. INCITS, TERMS OF REFERENCE FOR A STUDY PERIOD ON GUIDELINES FOR ELECTRONIC DISCOVERY, CS1-2012-00089-001.

30. ISO/IEC, REPORT OF THE 12TH MEETING OF ISO/IEC JTC 1/SC 27/WG 4, STOCKHOLM, SWEDEN, MAY 7TH–11TH, 2012, at 10, ISO/IEC JTC 1/SC 27 N 11000 (May 24, 2012).

31. *See* ISO/IEC, CALL FOR CONTRIBUTIONS TO THE WG 4 STUDY PERIOD IN THE AREA OF ELECTRONIC DISCOVERY, ISO/IEC JTC 1/SC 27 N11035 (July 6, 2012).

32. ISO/IEC, RESOLUTIONS OF THE 12TH SC 27 WG 4 PLENARY MEETING HELD IN STOCKHOLM, SWEDEN FROM 7–11 MAY, 2012/REVISION 1, at 11, ISO/IEC JTC 1/SC 27 N11309 (July 27, 2012).

33. INCITS, U.S. COMMENTS TO WG 4 STUDY PERIOD ON ELECTRONIC DISCOVERY, SC 27 N11035 (Sept. 21, 2012).

34. *See* SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM—FINAL REPORT ON PHASE TWO: MAY 2010–MAY 2012, *available at* http://www.discoverypilot.com/sites/default/files/Phase-Two-Final-Report-Appendix.pdf (last visited May 15, 2014).

35. *See* NYSBA, BEST PRACTICES IN E-DISCOVERY IN NEW YORK STATE AND FEDERAL COURTS (July 2011), *available at* http://www.nysba.org/Sections/Commercial_Federal_Litigation/ComFed_Display_Tabs/Reports/ediscoveryFinalGuidelines_pdf.html.

36. ISO/IEC, RESOLUTIONS OF THE 13TH MEETING OF ISO/IEC JTC 1/SC 27/WG 4 MEETING HELD IN ROME, ITALY, 2012-10-22 TO 2012-10-26, at 8, ISO/IEC JTC 1/SC 27 N11941 (Nov. 2, 2012).

provided contributions supporting an E-Discovery project with Australia arguing there was no need for such a project.[37] It was the consensus of the participating NBs and liaison organizations (i.e., China, United Kingdom, Italy, Japan, Korea, United States, and South Africa along with FIRST and INTERPOL) that there was a need for an NWIP in the area of E-Discovery.[38] Eric Hibbard and Angus Marshall were appointed the acting editors for the NWIP and tasked with developing the preliminary draft to be balloted by the NBs.[39]

Following the meeting in Rome, the editors prepared the NWIP, based on the contributions and decisions from the Study Period. This NWIP was then sent out in July 2013 by SC27 to the NBs as a three-month ballot, seeking approval of the project and soliciting comments and contributions on the NWIP.[40]

C. *The Road to Standardization Can Be Bumpy*

At the conclusion of the NWIP ballot in February 2013, Belgium, Brazil, China, Czech Republic, Italy, Korea, Mexico, Norway, Romania, Singapore, Slovakia, Slovenia, Thailand, United Kingdom, and United States voted to support the addition of E-Discovery to the SC27 program of work.[41] Unfortunately, only three NBs (Thailand, United Kingdom, and United States) indicated they were willing to participate in the project and identify at least one expert to be involved with the project.[42] Current ISO rules require a minimum of five NBs to both express a willingness to participate and identify experts.[43] Technically, the ballot did not pass—a bit of a surprise because seven NBs had indicated support during the Study Period. However, the final decision was deferred to the SC27 meeting in Sophia Antipolis, France, in April 2013.

Once at the SC27 meeting in Sophia Antipolis, the acting editors were able to do some lobbying of the NBs that had expressed support. In the end, both South Africa and Italy changed their positions in favor of participating

37. *See* ISO/IEC, SUMMARY OF NB CONTRIBUTIONS TO THE WG 4 STUDY PERIOD IN THE AREA OF ELECTRONIC DISCOVERY (IN RESPONSE TO SC 27 N11035), ISO/IEC JTC 1/SC 27 N11627 (Oct. 8, 2012).

38. ISO/IEC JTC 1/SC 27/WG 4 N 51, *supra* note 20, §§ 4.7–4.8.

39. ISO/IEC JTC 1/SC 27 N11941, *supra* note 36, at 14.

40. *See* ISO/IEC, NEW WORK ITEM PROPOSAL FOR ELECTRONIC DISCOVERY, ISO/IEC JTC 1/SC 27 N11955 (Nov. 5, 2012).

41. *See* ISO/IEC, SUMMARY OF VOTING ON SC 27 N11955—NEW WORK ITEM PROPOSAL ON ELECTRONIC DISCOVERY, at 2–3, ISO/IEC JTC 1/SC 27 N12221 (Feb. 8, 2013).

42. *Id.* at 4–5.

43. ISO/IEC DIRECTIVES, PART 1: CONSOLIDATED JTC 1 SUPPLEMENT 2014—PROCEDURES SPECIFIC TO JTC 1, 2013 ISO/IEC § 2.3.5.

in the project and identified experts, which resulted in the project being approved.[44] SC27/WG4 also formally appointed Eric Hibbard as the Project Editor and Angus Marshall as the Co-editor.[45]

At this point, it had been two years since the initial conversations about an E-Discovery standard had taken place. With the new ISO/IEC 27050 project on the "normal" development timeline (as opposed to the "extended" timeline), it would be at least three more years until the standard would be published.

III. A STANDARD IS "BORN"

With the ISO/IEC 27050 project approved, the real work commenced. The first Working Draft (WD) leveraged the materials from the NWIP, specifically the following scope statement:

> Electronic discovery (also known as eDiscovery and E-Discovery) is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or both parties involved in an investigation and any resulting actions. This International Standard addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of ESI. In addition, this International Standard provides guidance on measures, spanning from initial creation of ESI through its final disposition, which an organization can undertake to mitigate risk and expense should electronic discovery become an issue. This International Standard also identifies other relevant standards (e.g. ISO/IEC 27037) and how they relate to, and interact with, E-Discovery activities.
>
> This International Standard is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that this guidance is not intended to contradict or supersede local jurisdictional laws and regulations, so care should be exercised to ensure compliance with the prevailing jurisdictional requirements.[46]

Putting aside the standard's gibberish, this scope identified the E-Discovery processes (i.e., identification, preservation, collection, processing, review,

---

44. ISO/IEC, REVISED SUMMARY OF VOTING ON SC 27 N11955—NEW WORK ITEM PROPOSAL ON ELECTRONIC DISCOVERY (ISO/IEC NP 27050), at 4–5 ISO/IEC JTC 1/SC 27 N12633 (Apr. 23, 2013).

45. ISO/IEC, RESOLUTIONS 14TH WG 4 MEETING—RESOLUTIONS OF THE 14TH MEETING OF ISO/IEC JTC 1/SC 27/WG 4, HELD 2013-04-22 TO 2013-04-26, IN SOPHIA ANTIPOLIS, FRANCE, at 12, ISO/IEC JTC 1/SC 27/WG 4 N 184 (May 13, 2013).

46. ISO/IEC, TEXT 1STWD 27050—TEXT FOR ISO/IEC 1ST WD 27050, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—ELECTRONIC DISCOVERY, at 1, ISO/IEC JTC 1/SC 27/WG 4 N 233 (July 8, 2013).

analysis, and production, at a minimum) to be covered by the standard; it indicated that E-Discovery would be addressed in the broadest sense (e.g., investigations, records management, governance, legal, compliance, information technology, etc.); it would be relevant to a technical and non-technical audience (e.g., "non-technical personnel" was intended to mean lawyers and judges, managers, etc.); and it would focus on ESI (e.g., what it is, where it lives, how one protects it, etc.). This scope explicitly states that the standard would provide guidance (recommendations) on the full lifecycle of ESI, but interestingly, the scope did not state what it would do with the E-Discovery activities. This was by design because it was unclear at this early stage as to whether the standard would go beyond offering guidance and venture into the requirements space where compliance and conformance would became important.

The editors had roughly two months to prepare the ISO/IEC 1stWD 27050 text, which was expected to be distributed to the National Bodies in July 2013.[47] The primary focus for this version of the draft was to try to stabilize its structure, including conformance with the ISO standards template, and then to begin populating key sections (ISO calls them clauses) of the draft. Ignoring the typical sections included in ISO standards, Table 1 shows the major sections and sub-sections of the draft.

5	Overview
5.1	Background
5.2	Basic concepts
5.3	Objectives of electronic discovery
5.4	General principles of electronic discovery
6	Electronically Stored Information (ESI)
6.1	General
6.2	Common types of ESI
6.3	Common sources of ESI
6.4	ESI Representations
7	Electronic discovery process
7.1	General

47. ISO/IEC JTC 1/SC 27/WG 4 N 184, *supra* note 45, at 8.

7.2	Identification
7.3	Preservation
7.4	Collection
7.5	Processing
7.6	Review
7.7	Analysis
7.8	Production
8	Additional considerations
8.1	Electronic discovery readiness
8.2	Search technologies
8.3	Technology Assisted Reviews (TAR)
8.4	Avoiding data breaches

Table 1. Structure of ISO/IEC 1stWD 27050[48]

Most of the NWIP, which was based on the New York State Bar Association and Seventh Circuit E-Discovery materials, was integrated into this new structure. In addition, content from the *Good Practice Guide to Electronic Discovery in Ireland*[49] was used to supplement the United States materials. A conscious decision was made by the editor to not include guidance or requirements in this version of the draft standard. Last but not least, an effort was made to identify terminology (i.e., definitions) that could be used in the standard.[50]

NBs were given approximately ten weeks to prepare and submit their comments and contributions, which were due in mid-September 2013, and these in turn, were expected to be processed at the SC27 meeting in Incheon, South Korea, in October 2013.[51]

48. ISO/IEC JTC 1/SC 27/WG 4 N 233, *supra* note 46, at iii.

49. *Good Practice Guide to Electronic Discovery in Ireland*, EDISCOVERY GRP. OF IR. (Apr. 16, 2013), *available at* http://www.ediscoverygroup.ie.

50. ISO has explicit rules for including and formatting terms and definitions. There is also a desire to use existing definitions from other standards where possible.

51. ISO/IEC JTC 1/SC 27/WG 4 N 184, *supra* note 45, at 2.

A. *ISO "Doubles-down" on E-Discovery*

The number of comments received on the ISO/IEC 1stWD 27050 was relatively small (less than forty-five), but what they lacked in quantity, they made up for in quality.[52] The United States went into overdrive and provided one of the largest sets of contributions (exceeding 100 megabytes) ever submitted to SC27, and it included:

- New York State Bar Association (NYSBA), Best Practices in E-Discovery in New York State and Federal Courts, Version 2.0;[53]
- Full access to the Electronic Discovery Reference Model (EDRM) web-based materials;[54]
- Delaware Federal Court ESI Protocol;[55]
- Maryland Federal Court ESI Protocol;[56]
- Multiple documents from the Seventh Circuit's Electronic Discovery Pilot Program, including the Phase 2 Final Report, Phase 3 Interim Report, and the Principles Relating to the Discovery of Electronically Stored Information;[57] and
- Department of Justice, Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases.[58]

52. *See* ISO/IEC, SC27 SOC 1STWD 27050—SUMMARY OF COMMENTS RECEIVED ON SC 27 N12679, TEXT FOR ISO/IEC 1ST WD 27050, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—ELECTRONIC DISCOVERY, ISO/IEC JTC 1/SC 27/WG 4 N 275 (Sept. 18, 2013).

53. NYSBA, BEST PRACTICES IN E-DISCOVERY IN NEW YORK STATE AND FEDERAL COURTS VERSION 2.0 (Apr. 5, 2013), *available at* http://www.nysba.org/Sections/Commercial_Federal_Litigation/ComFed_Display_Tabs/Reports/Ediscovery_Final5_2013_pdf.html.

54. *Resources*, ELEC. DISCOVERY REFERENCE MODEL, http://www.edrm.net/ (last visited May 15, 2014) [hereinafter EDRM].

55. *See* DELAWARE FEDERAL COURTS, DEFAULT STANDARD FOR DISCOVERY INCLUDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION ("ESI") (Dec. 8, 2011), *available at* http://www.ded.uscourts.gov/sites/default/files/Chambers/SLR/Misc/EDiscov.pdf.

56. *See* U.S. DISTRICT COURT FOR THE DISTRICT OF MARYLAND, SUGGESTED PROTOCOL FOR DISCOVERY OF ELECTRONICALLY STORED INFORMATION ("ESI"), *available at* http://www.mdd.uscourts.gov/news/news/esiprotocol.pdf (last visited May 15, 2014).

57. *See* SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM—FINAL REPORT ON PHASE TWO, *supra* note 34; SEVENTH CIRCUIT ELECTRONIC DISCOVERY PILOT PROGRAM—INTERIM REPORT ON PHASE THREE: MAY 2012–MAY 2013, *available at* http://www.discoverypilot.com/sites/default/files/phase_three_interim_report.pdf (last visited May 15, 2014); 7th Circuit Elec. Discovery Comm., *Principles Relating to the Discovery of Electronically Stored Information*, DISCOVERY PILOT (Aug. 1, 2010), http://www.discoverypilot.com/sites/default/files/Principles8_10.pdf.

58. DEP'T OF JUST. & ADMIN. OFFICE OF THE U.S. COURTS JOINT WORKING GRP. ON ELEC. TECH. IN THE CRIM. JUST. SYS., RECOMMENDATIONS FOR ELECTRONICALLY STORED INFORMATION (ESI)

The problem with this type of input is that it was left as an exercise for the editors to figure out what it is and how it should be used. Such a scenario works well early in the project and when the editing team (editors and National Body participants) has extensive expertise. Unfortunately, few SC27 NBs have any depth of expertise in E-Discovery.

The large quantity of input, however, did have an immediate impact on the project. After reviewing the contributions, several NBs expressed concern that a single document would not be able to cover the breadth and complexity of E-Discovery.[59] Consequently, a decision was made to sub-divide the project so that different aspects of the topic (e.g., overview, governance/management, requirements, and technology issues) could be addressed in a more natural way, within an appropriate timeframe. Sub-dividing the project into multiple parts was expected to make it easier to maintain the standard and add new elements when appropriate.

While still in the SC27 meeting in Incheon, Korea, the editing team quickly converged on the following structure for the parts:

- ISO/IEC 27050-1, Information Technology—Security Techniques—Electronic Discovery—Part 1: Overview and Concepts
- ISO/IEC 27050-2, Information Technology—Security Techniques—Electronic Discovery—Part 2: Guidance for Governance and Management of Electronic Discovery
- ISO/IEC 27050-3, Information Technology—Security Techniques—Electronic Discovery—Part 3: Code of Practice for Electronic Discovery
- ISO/IEC 27050-4, Information Technology—Security Techniques—Electronic Discovery—Part 4: ICT Readiness for Electronic Discovery[60]

The expected interrelationship between these Parts is shown in Figure 1. Part 1 lays the foundation for the other Parts. Part 2 outlines the governance and management issues for E-Discovery. Part 3 provides the guidance and requirements associated with the E-Discovery process and activities. Part 4 addresses issues that may help organizations be better prepared to deal with E-Discovery.

DISCOVERY PRODUCTION IN FEDERAL CRIMINAL CASES (Feb. 2012), *available at* http://www.fd.org/docs/litigation-support/final-esi-protocol.pdf.

59. *See generally* ISO/IEC, RESOLUTIONS OF THE 15TH SC 27/WG 4 PLENARY MEETING, HELD 2013-10-21 TO 2013-10-25, INCHEON, KOREA, ISO/IEC JTC 1/SC 27/WG 4 N 372 (Jan. 2, 2014).

60. ISO/IEC, MOTIVATION FOR THE SUB-DIVISION OF ISO/IEC 27050, at 1–2, ISO/IEC JTC 1/SC 27/WG 4 N 360 (Nov. 13, 2013).

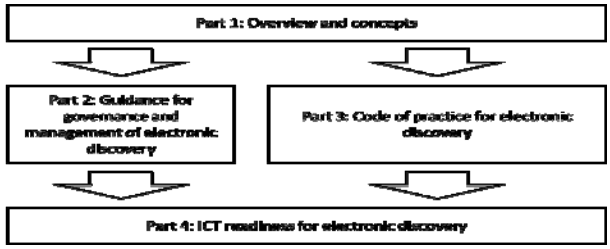

Figure 1. Relationship of ISO/IEC 27050 Parts[61]

With the sub-division of ISO/IEC 27050, SC27/WG4 significantly increased its E-Discovery workload as well as its need for editors to complete each of the projects. This was partially addressed by approving "extended" timelines for the development of Parts 2 to 4 (i.e., forty-eight-month development cycle).[62] To address the issues of editorship, the original editors were appointed as the leads (acting for Part 4), and a request for additional volunteers to serve as co-editors went out to the NBs.[63]

Because Part 1 was considered a continuation of the original ISO/IEC 1st WD 27050 work, its development cycle (thirty-six months) and stage were not changed. This was seen as a way of incentivizing the NBs to engage; in other words, by quickly progressing the E-Discovery concepts draft, those NBs that typically wait until the Committee Draft (CD) stage would be forced to review Part 1 while the other Parts were still at the WD stage, and it might serve as a catalyst to comment on the other Parts.

Coming out of the SC27 meeting in South Korea, the editors were tasked with using as much of the contributions against ISO/IEC 1stWD 270505 as possible to develop the four drafts and to submit them before the end of calendar year 2013.[64] NBs would then be asked to review and comment on the four parts in time for consideration at the SC27 meeting in Hong Kong in April 2014.[65]

B. *Part 1: Overview and Concepts*

Within SC27, most multi-part standards have an initial part (Part 1) that describes the structure of the standard and deals with terminology, concepts,

61. ISO/IEC, TEXT FOR ISO/IEC 2ND WD 27050-1, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—ELECTRONIC DISCOVERY—PART 1: OVERVIEW AND CONCEPTS, at 7, ISO/IEC JTC 1/SC 27/WG 4 N 387 (Jan. 16, 2014).

62. ISO/IEC JTC 1/SC 27/WG 4 N 372, *supra* note 59, at 10–11.

63. *Id.* at 11.

64. *Id.* at 2.

65. *Id.*

and other issues that span the various parts. In addition, an effort is made to avoid including guidance/recommendations or requirements (i.e., it is informative[66] rather than being normative[67]). ISO/IEC 27050-1 follows this model and provides an overview of E-Discovery, introducing relevant terminology, concepts, and processes; Part 1 is an informative document.

When a project is sub-divided, the scope clauses of each of the subsequent parts are typically subsets of the original scope. ISO/IEC 27050-1 is no different and the narrowed scope statement is:

> Electronic discovery is the process of discovering pertinent Electronically Stored Information (ESI) or data by one or both parties involved in an investigation and any resulting actions. This International Standard provides an overview of electronic discovery. In addition, it defines related definitions and describes the concepts, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of ESI. This International Standard also identifies other relevant standards (e.g., ISO/IEC 27037) and how they relate to, and interact with, electronic discovery activities.
>
> This International Standard is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities, and it is not intended to contradict or supersede local jurisdictional laws and regulations, so care should be exercised to ensure compliance with the prevailing jurisdictional requirements.[68]

Most of the content from the original ISO/IEC 1st WD 27050 was carried into the new Part 1 document, including the detail associated with ESI as well as describing the E-Discovery processes. A new clause was added to briefly describe the various parts in the standard and the "Additional Considerations" clause (as shown in Table 1) was replaced with new content (see Table 2).

---

66. Within the context of ISO standards, "informative" usually identifies supplemental information that helps with the conceptual understanding and often includes tutorials, commentary as well as background, history, development, and relationship with other elements; it is not a requirement and does not compel compliance.

67. ISO standards with normative language include requirements (denoted by the verbal form "shall"), recommendations (often denoted by the verbal form "should," "may," and "can"), and statements (including permissions, possibilities, and capabilities). In order to comply with the standard, it is necessary to comply only with the requirements.

68. ISO/IEC JTC 1/SC 27/WG 4 N 387, *supra* note 61, at 1.

9 Additional considerations
9.1 Information management
9.2 ESI presentation
9.3 Chain of custody and provenance
9.4 Protection of ESI

Table 2. Additional Consideration in ISO/IEC 2ndWD 27050-1[69]

One of the key challenges yet to be addressed in Part 1 is the conflict between the forensic-oriented terminology in ISO/IEC 27037 and the commonly used E-Discovery terminology. For example, the term *collection* is used in both disciplines, but they have very different meanings; forensic *acquisition* is a closer match to E-Discovery *collection*.

When completed, this document is expected to be a useful reference for E-Discovery and it is likely to be referenced by other ISO standards that must include material on E-Discovery.

C. *Part 2: Governance and Management*

When the sub-division of ISO/IEC 1st WD 27050 was being discussed, the United Kingdom was very insistent that one of the Parts needed to target C-level executives within organizations that may be confronted with E-Discovery scenarios, which may or may not be legal in nature. The concern was that E-Discovery should be conducted in a manner that conforms to the organization's governance requirements (e.g., compliance, privacy, etc.) and that it be managed proactively (e.g., covered by organizational policies).

The scope statement for Part 2 reflects these issues and it currently states:

> This international standard provides guidance for technical and non-technical personnel at senior levels within an organization, including those with responsibility for compliance with regulatory requirements, industry standards and, in some jurisdictions, legal requirements. It describes how such personnel can identify and take ownership of risks related to electronic discovery, set policy relating to electronic discovery and achieve compliance with external and internal requirements relating to electronic discovery. It also suggests how to produce such policies in a

69. *Id.* at IV.

> form which can advise process control. Furthermore, it provides guidance on how to implement and control electronic discovery in accordance with prevailing policies.[70]

There was very little relevant material in the ISO/IEC 1stWD 27050-2 document provided to the NBs for review. What little content that was contained in the draft leveraged the EDRM's Information Governance Reference Model (IGRM).[71] The role that E-Discovery plays within the context of information governance is expected to grow in importance, so Part 2 is expected to get much more attention by the SC27 NBs in the future.

D. *Part 3: Code of Practice*

Although the original ISO/IEC 1st WD 27050 contained no guidance, ultimately, this guidance was expected to be an important aspect of the standard. With the sub-division of the project, Part 3 was tagged as the document that would contain the bulk of the guidance, and more importantly, the requirements. The scope statement for ISO/IEC 1stWD 27050-3 is:

> This International Standard provides requirements and guidance on activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information (ESI). In addition, this International Standard specifies relevant measures that span the initial creation of ESI through its final disposition.
>
> This International Standard is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that this requirements [sic] and guidance is not intended to contradict or supersede local jurisdictional laws and regulations, so care should be exercised to ensure compliance with the prevailing jurisdictional requirements.[72]

In an effort to jumpstart the dialogue around E-Discovery guidance and requirements, the editors pulled extensive content from the EDRM[73] and the *Good Practice Guide to Electronic Discovery in Ireland*.[74] This approach

---

70. ISO/IEC, TEXT FOR ISO/IEC 1ST WD 27050-2, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—ELECTRONIC DISCOVERY—PART 2: GUIDANCE FOR GOVERNANCE AND MANAGEMENT OF ELECTRONIC DISCOVERY, at 1, ISO/IEC JTC 1/SC 27/WG 4 N 388 (Jan. 17, 2014).

71. *See Information Governance Reference Model*, EDRM, http://www.edrm.net/resources/guides/igrm (last visited May 15, 2014).

72. ISO/IEC, TEXT FOR ISO/IEC 1ST WD 27050-3, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—ELECTRONIC DISCOVERY—PART 3: CODE OF PRACTICE FOR ELECTRONIC DISCOVERY, at 1, ISO/IEC JTC 1/SC 27/WG 4 N 389 (Jan. 17, 2014).

73. *See* EDRM, *supra* note 54.

74. *See Good Practice Guide to Electronic Discovery in Ireland*, *supra* note 49.

had the advantage of providing a significant amount of content on the initial draft, but it definitely biased the content towards United States-style E-Discovery, as well as for larger organizations.

In the long run, Part 3 is expected to have the most impact on E-Discovery because of the inclusion of requirements that can serve as the basis for conformance.[75] Depending on the final form of the requirements, it may be possible to use them to certify an organization's E-Discovery practices, or they could serve as the evaluation criteria for professional certifications. At this point, however, it is difficult to fully understand how the requirements can and will be used because very few were included in the first WD.

E. *Part 4: ICT Readiness*

The final part resulting from the sub-division of ISO/IEC 1stWD 27050 is intended to address the E-Discovery technology issues.[76] For example, Part 3 provides guidance and requirements for the identification of ESI, and Part 4 could cover the ways an organization could do this in an efficient manner using a variety of tools and techniques. The scope statement for ISO/IEC 1stWD 27050-4 is:

> This International Standard provides guidance on the ways an organization can plan and prepare for, and implement, electronic discovery from the perspective of both technology and processes.
>
> This International Standard is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities. It is important to note that this guidance is not intended to contradict or supersede local jurisdictional laws and regulations, so care should be exercised to ensure compliance with the prevailing jurisdictional requirements.[77]

For this Part, it is all about the preparation and implementation of E-Discovery. It takes the policies and management from Part 2, combines it with the guidance and requirements for the E-Discovery processes and activities in Part 3, and provides guidance for the use of technology to make E-Discovery more effective and efficient.

As with Part 2, there was very little relevant material in the ISO/IEC 1stWD 27050-4 document that was provided to the NBs for review. This

---

75. *See* ISO/IEC JTC 1/SC 27/WG 4 N 372, *supra* note 59.

76. ISO/IEC JTC 1/SC 27/WG 4 N 387, *supra* note 61, at 8.

77. ISO/IEC, TEXT FOR ISO/IEC 1ST WD 27050-4, INFORMATION TECHNOLOGY—SECURITY TECHNIQUES—ELECTRONIC DISCOVERY—PART 4: ICT READINESS FOR ELECTRONIC DISCOVERY, at 1, ISO/IEC JTC 1/SC 27/WG 4 N 390 (Jan. 17, 2014).

was unfortunate, because the E-Discovery vendors are unlikely to focus on Part 4 as originally intended, and instead, they will focus on Part 3.

SUMMARY AND CONCLUSIONS

Starting in 2013, the discussions around whether an E-Discovery standard should be developed have been rendered moot with the approval of the SC27 ISO/IEC 27050 project. Since it is an international standard, there are likely to be differences from the United States approach to E-Discovery; however, multi-national organizations may benefit significantly from the consistency that it brings when dealing with cross-border issues.

The development of this new E-Discovery standard is taking place where most in the American legal community do not typically operate.[78] Organizations like the ABA EDDE Committee and the EDRM have found ways to engage as liaisons to the United States activities in INCITS/CS1,[79] but many other United States-based E-Discovery entities are not currently represented (e.g., a notable example is The Sedona Conference with its excellent E-Discovery body of knowledge).

The next round of ISO/IEC 27050 drafts are expected to be made available after the SC27 meeting in Hong Kong in April 2014; Part 1 will be available in early June 2014, and Parts 2 to 4 will be available in July 2014, with National Body comments and contributions due in mid-September 2014.[80] Interested United States parties can contact the INCITS/CS1 Storage and Evidence Ad Hoc Committee (storage_evidence@standards.incits.org) to explore ways to get involved.[81]

78. *Roster of INCITS Technical Committee CS1*, INCITS, https://standards.incits.org/apps/org/workgroup/cs1/members/roster.php.

79. For example, through membership in the cs1-us-ediscovery-edit-group@googlegroups.com Google Group, which is used by the Storage & Evidence Ad Hoc Committee of INCITS/CS1 for interaction with the United States legal community.

80. ISO/IEC, RESOLUTIONS OF THE 16TH SC 27/WG 4 PLENARY MEETING HELD 2014-04-07 TO 2014-04-11, HONG KONG, CHINA, at 2, ISO/IEC JTC 1/SC 27/WG 4 N 443 (Apr. 12, 2014).

81. *Charter of the Storage & Evidence Ad Hoc Committee of INCITS/CS1*, INCITS, https://standards.incits.org/apps/org/workgroup/storage_evidence/description.php.