Cybersecurity Partnership Meeting

United States Patent and Trademark Office
November 14, 2014 in Menlo Park, CA
Welcome

Mohammad H. Qayoumi
President of San Jose State University
Opening Remarks

Michelle Lee
Deputy Under Secretary of Commerce and Deputy Director of the USPTO
Overview of Cybersecurity Patent Initiatives

John Cabeca, Director, Silicon Valley USPTO
Nestor Ramirez, Director, Technology Center 2400
Kevin Stine
National Institute of Standards and Technology

United States Patent and Trademark Office
November 14, 2014 in Menlo Park, CA
Framework for Improving Critical Infrastructure Cybersecurity

US PTO Cybersecurity Partnership Meeting

November 14, 2014

Kevin Stine
Kevin.Stine@nist.gov
About NIST

- NIST’s mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
- 3,000 employees
- 2,700 guest researchers
- 1,300 field staff in partner organizations
- Two main locations: Gaithersburg, Md and Boulder, Co

NIST Priority Research Areas

- Advanced Manufacturing
- IT and Cybersecurity
- Healthcare
- Forensic Science
- Disaster Resilience
- Cyber-physical Systems
- Advanced Communications
The Role of NIST

- The National Institute of Standards and Technology’s mission is to stimulate innovation, foster industrial competitiveness, and improve the quality of life.

- Role in cybersecurity began in 1972 with the development of the Data Encryption Standard – began when commercial sector also has a legitimate need for cryptography, including in ATMs.

- Using widely-accepted standards helps create competitive markets around market need through combinations of price, quality, performance, and value to consumers. It then promotes faster diffusion of these technologies throughout industry.
Computer Security Division

The Computer Security Division provides standards and guidelines, tools, metrics, and practices to protect information and information systems.

Executive Order: Improving Critical Infrastructure Cybersecurity

“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties”

President Barack Obama
Executive Order 13636, Feb. 12, 2013

• The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
• Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work
Based on the Executive Order, the Cybersecurity Framework Must...

- Include a set of standards, methodologies, procedures, and processes that **align policy, business, and technological approaches to address cyber risks**

- Provide a **prioritized, flexible, repeatable, performance-based, and cost-effective approach**, including information security measures and controls, to help owners and operators of critical infrastructure **identify, assess, and manage cyber risk**

- **Identify areas for improvement** to be addressed through future collaboration with particular sectors and standards-developing organizations
The Cybersecurity Framework Is for Organizations...

- Of any size, in any sector in the critical infrastructure
- That already have a mature cyber risk management and cybersecurity program
- That don’t yet have a cyber risk management or cybersecurity program
- With a mission of helping keep up-to-date on managing risk and facing business or societal threats
It must apply from Executives to Operations

Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities

Mission Priority and Risk Appetite and Budget

Changes in Current and Future Risk

Business/Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget

Framework Profile

Implementation Progress
Changes in Assets, Vulnerability and Threat

Implementation/Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics.

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario.

Supports prioritization and measurement while factoring in business needs.

Cybersecurity activities and informative references, organized around particular outcomes.

Enables communication of cyber risk across an organization.

Framework Components

Framework Profile

Framework Core

Framework Implementation Tiers
## Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IDENTIFY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PROTECT</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DETECT</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RESPOND</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RECOVER</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**What assets need protection?**

**What safeguards are available?**

**What techniques can identify incidents?**

**What techniques can contain impacts of incidents?**

**What techniques can restore capabilities?**
### Framework Core - Sample

<table>
<thead>
<tr>
<th>Access Control (PR.AC)</th>
<th>PR.AC-1: Identities and credentials are managed for authorized devices and users</th>
<th>PR.AC-2: Physical access to assets is managed and protected</th>
<th>PR.AC-3: Remote access is managed</th>
</tr>
</thead>
</table>
| **PROTECT (PR)**        | • CCS CSC 16  
                          • COBIT 5 DSS05.04, DSS06.03  
                          • ISA 62443-2-1:2009 4.3.3.5.1  
                          • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9  
                          • NIST SP 800-53 Rev. 4 AC-2, IA Family | • COBIT 5 DSS01.04, DSS05.05  
                          • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8  
                          • NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 | • COBIT 5 APO13.01, DSS01.04, DSS05.03  
                          • ISA 62443-2-1:2009 4.3.3.6.6  
                          • ISA 62443-3-3:2013 SR 1.13, SR 2.6  
Framework Profile

- Alignment of **Functions, Categories, and Subcategories** with business requirements, risk tolerance, and resources of the organization

- Enables organizations to **establish a roadmap for reducing cybersecurity risk** that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities

- Can be used to describe **current state or desired target state** of cybersecurity activities
Framework Implementation Tiers

• Feedback indicated the need for the Framework to allow for flexibility in implementation and bring in concepts of maturity models.

• Responding to feedback, Framework Implementation Tiers were proposed to reflect how an organization implements the Framework Core functions and manages its risk.

• The Tiers are progressive, ranging from Partial (Tier 1) to Adaptive (Tier 4), with each Tier building on the previous Tier.

• The Tier characteristics are defined at the organizational level and are applied to the Framework Core to determine how a category is implemented.
How to Use the Cybersecurity Framework

The Framework is designed to complement existing business and cybersecurity operations, and can be used to:

- **Understand security status**
- **Establish / Improve a cybersecurity program**
- **Communicate cybersecurity requirements** with stakeholders, including partners and suppliers
- **Identify opportunities for new or revised standards**
- **Identify tools and technologies to help organizations use the Framework**
- **Integrate privacy and civil liberties considerations into a cybersecurity program**
What’s Next: Areas for Development, Alignment, and Collaboration

• The Executive Order calls for the framework to “identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations”

• High-priority areas for development, alignment, and collaboration were identified based on stakeholder input:
  • Authentication
  • Automated Indicator Sharing
  • Conformity Assessment
  • Cybersecurity Workforce
  • Data Analytics
  • Federal Agency Cybersecurity Alignment
  • International Aspects, Impacts, and Alignment
  • Supply Chain Risk Management
  • Technical Privacy Standards
What’s Next: Using the Cybersecurity Framework

- Organizations—led by their senior executives—are using the framework now

- Industry groups, associations, and non-profits are playing key roles in assisting their members to understand and use the framework by:
  - Building or mapping their sector’s specific standards, guidelines, and best practices to the framework
  - Developing and sharing examples of how organizations are using the framework

- NIST is committed to helping organizations understand and use the framework, getting feedback on initial use.

- Workshop was held on October 29th and 30th in Tampa, FL.
Key Points about the Framework

• It’s a framework, not a prescription
  • It provides a common language and systematic methodology for managing cyber risk
  • It does not tell an organization how much cyber risk is tolerable, nor does it claim to provide “the one and only” formula for cybersecurity
  • Having a common lexicon to enable action across a very diverse set of stakeholders will enable the best practices of elite organizations to become standard practices for everyone

• The framework is a living document
  • It is intended to be updated over time as stakeholders learn from implementation, and as technology and risks change
  • That’s one reason why the framework focuses on questions an organization needs to ask to manage its cyber risk. Practices, technology, and standards will change over time—principals will not
Established in 2012 as part of NIST’s Information Technology Laboratory, the NCCoE is dedicated to furthering innovation through rapid identification, integration, and adoption of practical, standards-based cybersecurity solutions.

The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across multiple sectors
- Narrow enough to be addressed through one or more reference designs built in NCCoE labs
- Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies

Operational Model focuses on two kinds of reference designs:

- Sector-specific use cases
- Sector-neutral building blocks (technology-specific)
Where to Learn More and Stay Current

The *Framework for Improving Critical Infrastructure Cybersecurity*, the *Roadmap*, and related news and information are available at:

- [http://www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)
- Email: [cyberframework@nist.gov](mailto:cyberframework@nist.gov)

National Cybersecurity Center of Excellence (NCCoE):

- [http://nccoe.nist.gov](http://nccoe.nist.gov)

Computer Security Resource Center:

Q&A
Nestor Ramirez
Director, Technology Center 2400

United States Patent and Trademark Office
November 14, 2014 in Menlo Park, CA
Cybersecurity Partnership

Information Session on Cybersecurity Patent Application and Examination

United States Patent and Trademark Office
November 14, 2014 in Menlo Park, CA
## Who Are We?

<table>
<thead>
<tr>
<th>1600</th>
<th>• Biotechnology and Organic Chemistry</th>
</tr>
</thead>
<tbody>
<tr>
<td>1700</td>
<td>• Chemical and Materials Engineering</td>
</tr>
<tr>
<td>2100</td>
<td>• Computer Architecture and Software</td>
</tr>
<tr>
<td>2400</td>
<td>• Networking, Multiplexing, Cable, and Security</td>
</tr>
<tr>
<td>2600</td>
<td>• Communications</td>
</tr>
<tr>
<td>2800</td>
<td>• Semiconductors, Electrical and Optical Systems and Components</td>
</tr>
<tr>
<td>2900</td>
<td>• Designs</td>
</tr>
<tr>
<td>3600</td>
<td>• Transportation, Construction, Electronic Commerce, Agriculture, National Security, and License &amp; Review</td>
</tr>
<tr>
<td>3700</td>
<td>• Mechanical Engineering, Manufacturing and Medical Devices/Processes</td>
</tr>
</tbody>
</table>
Information Security and Cryptography

- **Multiplexing**
  - Class: 370/All
  - AU: 2411-2413, 2451-2459, 2471-2479

- **Multicomputer Data Transferring (Networks)**
  - Class: 709/All
  - AU: 2441-2449, 2451-2459

- **Interactive Video Distribution**
  - Class: 725/All
  - AU: 2421, 2423-2427

- **Video signal processing for Television**

- **Cryptography Support**
  - Class: 713/All
  - AU: 2431-2439, 2491-2496

- **Information Security**
  - Class: 726/All
  - AU: 2431-2439, 2491-2496

- **Cryptography**
  - Class: 380/All
  - AU: 2431-2439, 2491-2496

- **Video Compression**
  - Class: 348/384-440, 699-702; 375/240.01-240.29
  - AU: 2482, 2483, 2485-2486

- **Television – Special Applications**
  - Class: 348/25-172, 618-643
  - AU: 2482, 2483, 2485-2486
Our Workforce - Information Security and Cryptography Art Units

*As of October 20, 2014
Our Workforce - Information Security and Cryptography Patent Examiners

*As of October 20, 2014
## Teleworking in TC 2400

<table>
<thead>
<tr>
<th>PROGRAMS</th>
<th>EXAMINERS and SPEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP10</td>
<td>156</td>
</tr>
<tr>
<td>PTP20</td>
<td>98</td>
</tr>
<tr>
<td>PTP32</td>
<td>162</td>
</tr>
<tr>
<td>PHP 50 MILES</td>
<td>187</td>
</tr>
<tr>
<td>PHP OUT 50M</td>
<td>24</td>
</tr>
<tr>
<td>TEAPP</td>
<td>147</td>
</tr>
<tr>
<td>PMTP</td>
<td>63</td>
</tr>
<tr>
<td>FMTP</td>
<td>16</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>853</strong></td>
</tr>
</tbody>
</table>

The pie chart illustrates the distribution of teleworking programs in TC 2400, with each sector representing a different program and its corresponding count of examiners and SPEs.
The Technology: Information Security and Cryptography

• Protection of system hardware, software, or data from maliciously causing destruction, unauthorized modification, or unauthorized disclosure.

• Subject matter relating to security policies, access control, monitoring, scanning data, countermeasures, usage control, data protection and user protection, e.g. privacy.

• Equipment and processes which (a) conceal or obscure intelligible information by transforming such information so as to make the information unintelligible to a casual or unauthorized recipient, or (b) extract intelligible information from such a concealed representation, including breaking of unknown codes and messages.
The Technology: Cooperative Patent Classification (CPC)

Information Security - Cryptography

Platform Protection  Virus Detection  Access Control

Storage/ Memory/Carrier Security

G06F 21/00

Symmetric Key  Firewalls / Intrusion Detection  Vulnerability Testing

Public Key / Signature Systems  VPN

H04L 9/00  H04W 12/00

H04L 63/00
Information Security and Cryptography Applications - Filed vs. Issued

<table>
<thead>
<tr>
<th></th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Security Applications Filed</td>
<td>5297</td>
<td>6582</td>
<td>7577</td>
<td>5378</td>
</tr>
<tr>
<td>Number of Security Applications Issued</td>
<td>3277</td>
<td>4433</td>
<td>5818</td>
<td>5885</td>
</tr>
</tbody>
</table>

*Filing numbers for 2014 reflects partial data
# Filing - Top 15 Assignees

Information Security and Cryptography Applications

<table>
<thead>
<tr>
<th>No. Apps</th>
<th>Assignee</th>
<th>No. Apps</th>
<th>Assignee</th>
<th>No. Apps</th>
<th>Assignee</th>
<th>No. Apps</th>
<th>Assignee</th>
<th>No. Apps</th>
<th>Assignee</th>
</tr>
</thead>
<tbody>
<tr>
<td>210</td>
<td>IBM</td>
<td>297</td>
<td>IBM</td>
<td>373</td>
<td>IBM</td>
<td>173</td>
<td>IBM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>199</td>
<td>Microsoft</td>
<td>214</td>
<td>Google</td>
<td>153</td>
<td>Intel</td>
<td>103</td>
<td>Symantec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>Google</td>
<td>137</td>
<td>Microsoft</td>
<td>152</td>
<td>Google</td>
<td>71</td>
<td>Google</td>
<td></td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>Symantec</td>
<td>125</td>
<td>EMC</td>
<td>145</td>
<td>Amazon</td>
<td>67</td>
<td>Microsoft</td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>McAfee</td>
<td>123</td>
<td>Intel</td>
<td>120</td>
<td>Symantec</td>
<td>64</td>
<td>Samsung</td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>EMC</td>
<td>91</td>
<td>Symantec</td>
<td>114</td>
<td>EMC</td>
<td>60</td>
<td>Amazon</td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Apple</td>
<td>90</td>
<td>Samsung</td>
<td>111</td>
<td>Microsoft</td>
<td>50</td>
<td>Bank of America</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>Amazon</td>
<td>87</td>
<td>Amazon</td>
<td>91</td>
<td>Samsung</td>
<td>46</td>
<td>Qualcomm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>ETRI</td>
<td>81</td>
<td>Toshiba</td>
<td>83</td>
<td>Qualcomm</td>
<td>45</td>
<td>Tencent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>Samsung</td>
<td>78</td>
<td>Blackberry</td>
<td>76</td>
<td>Toshiba</td>
<td>39</td>
<td>Toshiba</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Toshiba</td>
<td>50</td>
<td>Cisco</td>
<td>66</td>
<td>Cisco</td>
<td>34</td>
<td>EMC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Sony</td>
<td>49</td>
<td>HP</td>
<td>66</td>
<td>HP</td>
<td>33</td>
<td>Huawei</td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>HP</td>
<td>49</td>
<td>ETRI</td>
<td>48</td>
<td>Fujitsu</td>
<td>32</td>
<td>Sony</td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Cisco</td>
<td>47</td>
<td>Sony</td>
<td>47</td>
<td>NEC</td>
<td>31</td>
<td>Intuit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>RIM</td>
<td>46</td>
<td>Broadcom</td>
<td>46</td>
<td>Tencent</td>
<td>31</td>
<td>Intel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Filing numbers for 2014 reflects partial data*
# Filing - Top 15 Countries
Information Security and Cryptography Applications  
(by Country of Assignee)

<table>
<thead>
<tr>
<th>No. Apps</th>
<th>Assignee</th>
<th>No. Apps</th>
<th>Assignee</th>
<th>No. Apps</th>
<th>Assignee</th>
<th>No. Apps</th>
<th>Assignee</th>
<th>No. Apps</th>
<th>Assignee</th>
</tr>
</thead>
<tbody>
<tr>
<td>415</td>
<td>Japan</td>
<td>413</td>
<td>Japan</td>
<td>501</td>
<td>Japan</td>
<td>277</td>
<td>Japan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>189</td>
<td>Korea</td>
<td>229</td>
<td>Korea</td>
<td>243</td>
<td>Korea</td>
<td>161</td>
<td>Korea</td>
<td></td>
<td></td>
</tr>
<tr>
<td>132</td>
<td>France</td>
<td>166</td>
<td>China</td>
<td>199</td>
<td>China</td>
<td>139</td>
<td>China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>China</td>
<td>135</td>
<td>France</td>
<td>125</td>
<td>Germany</td>
<td>87</td>
<td>Germany</td>
<td></td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>Canada</td>
<td>133</td>
<td>Canada</td>
<td>108</td>
<td>France</td>
<td>51</td>
<td>Taiwan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>Germany</td>
<td>127</td>
<td>Germany</td>
<td>104</td>
<td>Taiwan</td>
<td>51</td>
<td>Canada</td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>Finland</td>
<td>76</td>
<td>Taiwan</td>
<td>94</td>
<td>Canada</td>
<td>46</td>
<td>France</td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>Taiwan</td>
<td>74</td>
<td>United Kingdom</td>
<td>65</td>
<td>Israel</td>
<td>40</td>
<td>Finland</td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>Sweden</td>
<td>56</td>
<td>Finland</td>
<td>57</td>
<td>United Kingdom</td>
<td>36</td>
<td>Netherlands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Netherlands</td>
<td>49</td>
<td>Sweden</td>
<td>57</td>
<td>Sweden</td>
<td>34</td>
<td>United Kingdom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>United Kingdom</td>
<td>35</td>
<td>Israel</td>
<td>50</td>
<td>Finland</td>
<td>31</td>
<td>Israel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Israel</td>
<td>30</td>
<td>Netherlands</td>
<td>34</td>
<td>Russian Federation</td>
<td>30</td>
<td>Russian Federation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Switzerland</td>
<td>26</td>
<td>Russian Federation</td>
<td>31</td>
<td>Netherlands</td>
<td>21</td>
<td>Sweden</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Russian Federation</td>
<td>23</td>
<td>Switzerland</td>
<td>31</td>
<td>Cayman Islands</td>
<td>18</td>
<td>Switzerland</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Filing numbers for 2014 reflects partial data*
## Filing - Top 15 U.S. States
### Information Security and Cryptography Applications
(by U.S. state of Assignee)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>987</td>
<td>CA</td>
<td></td>
<td>1278</td>
<td>CA</td>
<td>1531</td>
<td>CA</td>
<td>816</td>
<td>CA</td>
</tr>
<tr>
<td>290</td>
<td>NY</td>
<td></td>
<td>392</td>
<td>NY</td>
<td>483</td>
<td>NY</td>
<td>243</td>
<td>NY</td>
</tr>
<tr>
<td>278</td>
<td>WA</td>
<td></td>
<td>214</td>
<td>WA</td>
<td>206</td>
<td>TX</td>
<td>108</td>
<td>TX</td>
</tr>
<tr>
<td>144</td>
<td>MA</td>
<td></td>
<td>193</td>
<td>MA</td>
<td>187</td>
<td>MA</td>
<td>90</td>
<td>WA</td>
</tr>
<tr>
<td>137</td>
<td>TX</td>
<td></td>
<td>169</td>
<td>TX</td>
<td>171</td>
<td>NV</td>
<td>75</td>
<td>MA</td>
</tr>
<tr>
<td>92</td>
<td>NJ</td>
<td></td>
<td>110</td>
<td>NV</td>
<td>164</td>
<td>WA</td>
<td>72</td>
<td>NC</td>
</tr>
<tr>
<td>80</td>
<td>NV</td>
<td></td>
<td>108</td>
<td>NJ</td>
<td>116</td>
<td>GA</td>
<td>72</td>
<td>GA</td>
</tr>
<tr>
<td>79</td>
<td>IL</td>
<td></td>
<td>98</td>
<td>IL</td>
<td>107</td>
<td>NJ</td>
<td>64</td>
<td>NV</td>
</tr>
<tr>
<td>72</td>
<td>NC</td>
<td></td>
<td>74</td>
<td>DE</td>
<td>100</td>
<td>FL</td>
<td>64</td>
<td>NJ</td>
</tr>
<tr>
<td>58</td>
<td>DE</td>
<td></td>
<td>69</td>
<td>NC</td>
<td>97</td>
<td>IL</td>
<td>57</td>
<td>IL</td>
</tr>
<tr>
<td>55</td>
<td>GA</td>
<td></td>
<td>68</td>
<td>VA</td>
<td>71</td>
<td>VA</td>
<td>40</td>
<td>FL</td>
</tr>
<tr>
<td>53</td>
<td>VA</td>
<td></td>
<td>66</td>
<td>GA</td>
<td>57</td>
<td>NC</td>
<td>31</td>
<td>PA</td>
</tr>
<tr>
<td>31</td>
<td>PA</td>
<td></td>
<td>50</td>
<td>FL</td>
<td>49</td>
<td>DE</td>
<td>25</td>
<td>VA</td>
</tr>
<tr>
<td>28</td>
<td>CO</td>
<td></td>
<td>38</td>
<td>CO</td>
<td>37</td>
<td>PA</td>
<td>22</td>
<td>MD</td>
</tr>
<tr>
<td>27</td>
<td>FL</td>
<td></td>
<td>37</td>
<td>MD</td>
<td>33</td>
<td>KS</td>
<td>21</td>
<td>KS</td>
</tr>
</tbody>
</table>

*Filing numbers for 2014 reflects partial data*
### Pendency Metrics – FY 2014
Information Security and Cryptography Applications

<table>
<thead>
<tr>
<th>Security Patent Applications</th>
<th>Pendency</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Action Pendency (Average number of months between filing date and first action)</td>
<td>16.14 months</td>
</tr>
<tr>
<td>Total Action Pendency (Average number of months between filing date and issue or abandonment)</td>
<td>29.04 months</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Patent Applications</th>
<th>Percentage of Actions within 4 months</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amendments</td>
<td>93.4%</td>
</tr>
<tr>
<td>RCE</td>
<td>50.1%</td>
</tr>
<tr>
<td>Patent Trial and Appeal Board (PTAB)</td>
<td>99.0%</td>
</tr>
</tbody>
</table>
### Appeal Metrics

Information Security and Cryptography Applications

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Appeal Briefs Filed</td>
<td>243</td>
</tr>
<tr>
<td>Examiner’s Answers</td>
<td>296</td>
</tr>
<tr>
<td>Abandonment after Board Decision</td>
<td>228</td>
</tr>
<tr>
<td>Allowance after Board Decision</td>
<td>105</td>
</tr>
<tr>
<td>Reopened after Board Decision</td>
<td>8</td>
</tr>
</tbody>
</table>

#### Board Decisions

- **Affirmance**: 65%
- **Reversal**: 22%
- **Affirmed in Part**: 13%

- **Total**: 100%
Quality Metrics: Quality Index Report (QIR)

- Quality Index Report (QIR) is a measure of the degree to which actions in the prosecution of all patent applications reveal trends indicative of quality concerns.

- This index is based on data currently available through the USPTO’s Patent Application Locating and Monitoring (PALM) internal tracking system.

- This index is calculated by statistical analysis of occurrences of certain types of events as recorded in PALM.
<table>
<thead>
<tr>
<th>Quality Index Report (QIR) Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actions Per Disposal</strong></td>
</tr>
<tr>
<td>% employees averaging less than 3 actions per disposal</td>
</tr>
<tr>
<td><strong>RCEs of Total Disposals</strong></td>
</tr>
<tr>
<td>% disposals that are not RCEs</td>
</tr>
<tr>
<td><strong>Reopenings After Final</strong></td>
</tr>
<tr>
<td>% final actions not reopened</td>
</tr>
<tr>
<td><strong>Non-FAOM Non-Final Actions</strong></td>
</tr>
<tr>
<td>% non-final actions that are not second or subsequent non-final actions</td>
</tr>
<tr>
<td><strong>Restrictions After First Action</strong></td>
</tr>
<tr>
<td>% total restrictions not made on second or subsequent action</td>
</tr>
</tbody>
</table>
Quality Metrics: Quality Index Report
Information Security and Cryptography Examinations

Emp avg <3 actions per disposal
%Disposals not RCE
%Finals not reopened
%total actions not 2nd+ non-final
%Restrictions not made after FAOM
The Centralized Patent Application Initiative website is a single online location highlighting the advantages of various patent programs available to applicants during specific stages of prosecution.
# Patent Application Initiatives (PAI) Website

## USPTO Patent Application Initiatives Timeline

<table>
<thead>
<tr>
<th>FILING</th>
<th>FIRST ACTION</th>
<th>FINAL REJECTION</th>
<th>APPEAL</th>
<th>ALLOWANCE</th>
<th>ISSUE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ADVANCEMENT OF EXAMINATION OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Track One - Prioritized Examination</td>
<td>After Final Consideration Pilot 2.0 (AFCP 2.0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accelerated Examination</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full First Action Interview Pilot</td>
<td>Pre-Appeal Program</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patent Prosecution Highway (PPH 2.0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCT Patent Prosecution Highway (PCT PPH 2.0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Glossary Pilot</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Petition to Make Special</td>
<td>Petition to Make Special</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ombudsman Program</td>
<td>Ombudsman Program</td>
<td></td>
<td>Ombudsman Program</td>
<td>Ombudsman Program</td>
<td></td>
</tr>
<tr>
<td><strong>INTERVIEW OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Interview Practice</td>
<td>General Interview Practice</td>
<td>General Interview Practice</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>INFORMATION DISCLOSURE STATEMENT (IDS) OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS - No Certification or Fee</td>
<td>IDS - Certification or Fee</td>
<td>IDS - Certification and Fee</td>
<td>IDS - Certification and Fee</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Quick Path Information Disclosure Statement (QPIDS)
Navigating the PAI Website

USPTO Patent Application Initiatives - Prior to Examination

<table>
<thead>
<tr>
<th>Description</th>
<th>Track One (Prioritized Examination)</th>
<th>Accelerated Examination</th>
<th>Full First Action Interview Pilot</th>
<th>Patent Prosecution Highway (PPH 2.0)</th>
<th>PCT Patent Prosecution Highway (PCT PPH 2.0)</th>
<th>Glossary Pilot</th>
<th>Ombudsman Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>The goal is to provide a final disposition within twelve months, on average, of prioritized status being granted. Learn about Track One statistics.</td>
<td>Accelerated examination provides applicant the opportunity to have final disposition of an application in 12 months. Learn about Accelerated Examination statistics</td>
<td>Under this Program, an applicant is entitled to a first action interview upon request, prior to the first Office action on the merits.</td>
<td>An applicant receiving a ruling from the Office of First Filing (OFF) that at least one claim in an application filed in the OFF is patentable may request that the Office of Second Filing (OSF) learn about PPH Statistics</td>
<td>European Patent Office (EPO) or the USPTO may request that the other office fast track the examination of corresponding claims in corresponding applications.</td>
<td>Focus on enhancing claim clarity in the specification of software-related applications through the use of glossaries.</td>
<td>The Patent Ombudsman Program enhances the USPTO’s ability to assist applicants or their representatives with issues that arise during patent application prosecution.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently Active (accepting applications)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes, extended beyond 11/16/12</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (as of 05/02/14)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

** Petition / Request:

- Request
- Petition
- Request
- Petition
- Request
- Petition

---

** if claims are in condition for allowance, no interview is required

** if extension of time is filed, application is out of Track One

*** no fee if statement of claimed subject matter is directed to environmental quality, energy, or countering terrorism
### Patent Application Initiatives

Information Security and Cryptography Applications

<table>
<thead>
<tr>
<th>Year</th>
<th>Track One</th>
<th>Patent Prosecution Highway</th>
<th>Accelerated Exam</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Granted</td>
<td>Denied</td>
<td>Granted</td>
</tr>
<tr>
<td>FY2014</td>
<td>286</td>
<td>0</td>
<td>27</td>
</tr>
<tr>
<td>FY2013</td>
<td>210</td>
<td>0</td>
<td>33</td>
</tr>
<tr>
<td>FY2012</td>
<td>164</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>FY2011</td>
<td>N/A</td>
<td>N/A</td>
<td>23</td>
</tr>
</tbody>
</table>
Patent Application Initiatives: Pendency to First Office Action
Information Security and Cryptography Applications

*no data for Track One requests for FY 2011
Patent Application Initiatives: Allowance Rate
Information Security and Cryptography Applications

*no data for Track One requests for FY 2011

*no data for Track One requests for FY 2011
Patent Application Initiatives:
Quick Path Information Disclosure Statement (QPIDS)

- Features of the QPIDS:
  - A QPIDS submission may only be filed after payment of the issue fee and before issuance of the patent.
  - The following items are included in a QPIDS submission:
    - A QPIDS transmittal form, PTO/SB/09.
    - An IDS, including a timeliness statement as set forth in 37CFR 1.97(e) and the IDS fee set forth in 37 CFR 1.17(p).
    - A Web-Based ePetition to withdraw from issue under 37 CFR 1.313(c)(2), and the petition fee set forth in 37 CFR 1.17(h).
    - A RCE and the RCE fee under 37 CFR 1.17(e).
    - An authorization to charge all fees associated with the QPIDS to a USPTO deposit account.
• Features of the QPIDS (cont.):

  – If the examiner determines that the QPIDS necessitated reopening prosecution, the Office will issue a form PTO-2300, titled “Notification of Reopening of Prosecution Due to Consideration of An Information Disclosure Statement Filed After Mailing of A Notice of Allowance,” and the RCE will be processed.

  – Otherwise, the Office will issue a corrected notice of allowability (PTO-37), which will identify the IDS and be accompanied by a copy of the submitted IDS listing as considered by the examiner.
## Patent Application Initiatives: QPIDS Metrics

### Technology Center 2400

<table>
<thead>
<tr>
<th></th>
<th>FY 12</th>
<th>FY 13</th>
<th>FY 14</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of QPIDS Filed and Completed Process</td>
<td>31</td>
<td>97</td>
<td>231</td>
<td>359</td>
</tr>
<tr>
<td>• # Corrected NOAs mailed</td>
<td>29</td>
<td>92</td>
<td>202</td>
<td>323</td>
</tr>
<tr>
<td>• Total # of RCEs processed</td>
<td>2</td>
<td>5</td>
<td>29</td>
<td>36</td>
</tr>
</tbody>
</table>

### Security Workgroups 2430 and 2490

<table>
<thead>
<tr>
<th></th>
<th>FY 12</th>
<th>FY 13</th>
<th>FY 14</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of QPIDS Filed and Completed Process</td>
<td>11</td>
<td>37</td>
<td>38</td>
<td>86</td>
</tr>
<tr>
<td>• # Corrected NOAs mailed</td>
<td>10</td>
<td>34</td>
<td>33</td>
<td>77</td>
</tr>
<tr>
<td>• Total # of RCEs processed</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>9</td>
</tr>
</tbody>
</table>

## FY 2012 – FY 2014
Features of the AFCP 2.0:

- Applicants must request entry into AFCP 2.0

- Applicants must submit an amendment to at least one independent claim that does not broaden the scope of the independent claim.

- If the application is not allowed, the examiner must request an interview with the applicant in order to claim non-production time.
% RCEs With No Prior After Final Communication - TC 2400
### Percentage of Subsequent Appeal Briefs in AFCP 2.0 and Non-AFCP 2.0 Applications - TC 2400

<table>
<thead>
<tr>
<th>Application Type</th>
<th>Number of Cases</th>
<th>% of Total Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-AFCP 2.0 After-final Applications With Subsequent Appeal Brief</td>
<td>830</td>
<td>6.2%</td>
</tr>
<tr>
<td>AFCP 2.0 Applications with Subsequent Appeal Brief</td>
<td>106</td>
<td>1.7%</td>
</tr>
</tbody>
</table>

(May 19, 2013* – October 20, 2014)

*Start Date of AFCP 2.0
Preliminary External Survey Results:

- When asked if the AFCP 2.0 reduced the likelihood an RCE will be filed in the application, 62% responded affirmatively.
- 75% of respondents felt that the AFCP 2.0 is either somewhat or very effective in advancing prosecution.
- Respondents were 3 times more likely to recommend continuation of the AFCP 2.0 than otherwise.
- Consistency of AFCP 2.0 implementation and examiner familiarity with the AFCP 2.0 were two concerns of respondents.
  - Additional training has been provided to examiners.
  - Examiner/SPE access to Patent Application Initiatives (PAI).
29.8% of Serial Disposals completed in September 2014 had at least one interview.
Questions and Comments?

Nestor Ramirez
Director, TC2400
Nestor.Ramirez@uspto.gov
Break
Alice Corp. v. CLS Bank
Legal Landscape since Alice Corp. and USPTO §101 Guidelines

Angela Ziegenhorn, Senior Director IP, Symantec
Michael Cygan, Legal Advisor, OPLA
Thoughts on the Impact of *Alice v. CLS Bank* on Security Software Patents

Angela Ziegenhorn
Senior Director IP
Symantec Corporation
Alice v. CLS Bank In a Nutshell

- In *Alice*, the Supreme Court:
  - Affirmed its judicial-exception approach to 35 U.S.C. § 101
  - Applied the two step framework from *Mayo* to computer implemented inventions
  - But limited its decision to the facts of the case, without defining “abstract idea” or making categorical rules
- *Alice* maintains ambiguity about the scope of the abstract idea exception
- Ambiguity makes property rights and investment risky and uncertain, potentially inhibiting business
- The Supreme Court recognized this danger
  - “At the same time, we tread carefully in construing this exclusionary principle lest it swallow all of patent law.” *Alice Corp. Pty. Ltd. v. CLS Bank Intern.*, 134 S.Ct. 2347, 2354 (2014)
Applying Alice: Step 1

- Step 1: “First, we determine whether the claims at issue are directed to [a] patent-ineligible [abstract idea].”
  - *Alice Corp. Pty. Ltd. v. CLS Bank Intern.*., 134 S.Ct. 2347, 2355 (2014)
- But *Alice* provides no real clarity on how to make this determination and relies instead on comparisons to prior cases
  - Looking at the case law, if an applicant’s claims are closer to *Benson, Flook, Bilski,* and *Alice,* then the claims are less likely to be subject-matter eligible; more likely if closer to the rubber-curing method in *Diehr*
- Commentators have various views of what *Alice* might mean
  - Professor Chisum proposed that a claim is not abstract under *Alice* if it presents a “novel and unobvious solution to a technical problem”
  - Another commentator suggested that *Alice* applies only to abstract ideas that are “fundamental practices long prevalent in their fields”, like hedging
Applying Alice: Step 2

- **Step 2:** We then conduct a “search for an ‘inventive concept’ — *i.e.*, an element or combination of elements that is ‘sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [abstract idea] itself.’”
  - *Alice Corp. Pty. Ltd. v. CLS Bank Intern.,* 134 S.Ct. 2347, 2355 (2014)
- In discussing this step, the Supreme Court provided us with a new useful “clue”
  - Per the Supreme Court, the *Alice* claims were invalid because “they do not, for example, purport to improve the functioning of the computer itself or effect an improvement in any other technology or technical field.”
  - The Supreme Court wrote “for example” because this “technology” test is just one factor, not a per se rule.
  - The Solicitor General argued that this “technology” test should be a per se requirement. Similarly, the *Alice* concurrence argued for a per se rule against business method patents.
  - The controlling majority of the Supreme Court declined to adopt either per se rule.
How Are Federal Courts Interpreting *Alice*?

- Aggressively!
- Of the first 20 decisions applying *Alice*, the courts have invalidated claims in 16 of them
  - Three invalidations affirmed at the Federal Circuit
  - All invalidations occurred before trial (e.g., at the motion to dismiss, judgment on the pleadings, or summary judgment stage)
- Among patents with invalidated claims:
  - Three directed to software
  - 10 directed to simple business methods, games, and ways of organizing human behavior (meal plans, Bingo, etc.)
  - One directed to pure databases
  - Two directed to medical information/diagnostics
- Even when claims survive one stage of litigation (e.g., motion to dismiss), judges indicate that they remain vulnerable under *Alice* at later stages (e.g., summary judgment)
USPTO’s Response to Alice

- Issued a memo of preliminary instructions to the examining corps.
- Issued the first final written decision, in a Covered Business Method trial, that applies Alice to invalidate a patent
- Withdrew some allowances due to Alice
  - [http://www.uspto.gov/blog/director/entry/update_on_uspto_s_implementation](http://www.uspto.gov/blog/director/entry/update_on_uspto_s_implementation)
- Issuing 101 Rejections
Applying *Alice* to Security Software: Step 1

- Is security software an “abstract idea?”
  - Security software compares very favorably with prior Supreme Court decisions on abstract ideas.
  - Security software typically focuses on real-world applications of mathematical and other algorithms, as was the case in *Diehr*.
  - Security software often protects vulnerabilities of particular platforms or networks (operating systems, firmware, protocols, etc.) and is designed to act on physical systems, just as the software in *Diehr*.
  - Security software is thus much closer in kind to the rubber curing method in *Diehr* than the pure binary mathematical operation in *Benson* or the fundamental economic practices (hedging and intermediated settlement) in *Bilski* and *Alice*.
    - Security software also typically does not rely solely on the alleged novelty of pure mathematical algorithms to ensure patentability, unlike the method in *Flook*, which relied on the alleged novelty of a mathematical “smoothing” function.
Applying *Alice* to Security Software: Step 2

- Even if one concludes that a security software patent is directed to an “abstract idea,” can the claims still recite an “inventive concept” that is sufficient to make the claims patent-eligible?
- The new useful “clue” from *Alice* results in a very favorable interpretation
  - Security software typically improves the reliability, stability, efficiency, and/or security of computing devices, thus satisfying the Supreme Court’s example of something that “improve[s] the functioning of the computer itself”
  - These characteristics are a strong indication that security software represents patent-eligible subject matter
Thoughts on Drafting Valid Security Software Patent Claims

- Avoid overly broad claims (e.g., provide context in a claim for how an algorithm or process will be used)
- Focus on how a security process interacts with the software and hardware platforms/networks it protects
- Craft claims and specifications that show how security processes improve the functionality of computing devices and/or networks
Thank You

Angela Ziegenhorn
Angela_Ziegenhorn@Symantec.com
APPENDIX
## Federal Court Decisions Applying Alice

<table>
<thead>
<tr>
<th>Software</th>
<th>Simple Business Method</th>
<th>Pure Database</th>
<th>Medical Infor.</th>
<th>Invalidate</th>
<th>Survive</th>
<th>Motion to Dismiss</th>
<th>Judg. on the Pleadings</th>
<th>Summary Judg.</th>
<th>Federal Circuit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amdocs</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Autoform</td>
<td>X (mechanical)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BuySafe</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Card Verificat.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cogent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comcast</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Data Distrib.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diet Goal</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digitech Image</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Eclipse</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Every Penny</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Genetic Tech.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Federal Court Decisions Applying Alice

<table>
<thead>
<tr>
<th>Software</th>
<th>Simple Business Method</th>
<th>Pure Database</th>
<th>Medical Infor.</th>
<th>Invalidate</th>
<th>Survive</th>
<th>Motion to Dismiss</th>
<th>Judg. on the Pleadings</th>
<th>Summary Judg.</th>
<th>Federal Circuit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helios</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hitkansut</td>
<td>X (mechanical)</td>
<td></td>
<td></td>
<td>X (in part)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Loyalty</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>MCRO</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Open Text</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planet Bingo</td>
<td>X (game)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Tuxis</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Walker Digital</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>5</td>
<td>11</td>
<td>2</td>
<td>2</td>
<td>16</td>
<td>4</td>
<td>7</td>
<td>4</td>
<td>9</td>
</tr>
</tbody>
</table>
Cybersecurity Partnership
Menlo Park, CA
November 14, 2014

*Alice Corp. v. CLS Bank*
USPTO Preliminary Examination
Instructions 2014

Michael Cygan
Senior Legal Advisor
Office of Patent Legal Administration
Subject Matter Eligibility

• Supreme Court has issued four decisions on subject matter eligibility in the last five years:

2010: *Bilski v. Kappos*
  – Method claims directed to abstract ideas.

2012: *Mayo v. Prometheus*
  – Method claims directed to laws of nature.

2013: *Association for Molecular Pathology v. Myriad Genetics*
  – Product claims directed to natural phenomena (“products of nature”).

2014: *Alice Corp. v. CLS Bank*
  – Method and product claims directed to abstract ideas.
Summary of *Alice Corp. v. CLS Bank*

- Alice Corp. is the assignee of the four patents at issue. The patents include method, computer system and computer readable storage medium claims.
  - The invention is directed to a scheme for mitigating “settlement risk,” *i.e.*, the risk that only one party to an agreed-upon financial exchange will satisfy its obligation, in which a computer system is used as a third-party intermediary between the parties to the exchange.
  - The claims were found ineligible because “the claims at issue amount to ‘nothing significantly more’ than an instruction to apply the abstract idea of intermediated settlement using some unspecified, generic computer.”
Impact of *Alice Corp.* on the Subject Matter Eligibility Analysis

- **The decision in *Alice Corp.* does:**
  - follow the analytical framework set forth by the Supreme Court in *Mayo*.
  - extend the *Mayo* framework to all types of claims and all types of judicial exceptions.

- **The decision in *Alice Corp.* does not:**
  - create a *per se* excluded category of subject matter, such as software or business methods, or
  - impose any special requirements for eligibility of software or business methods.
Alice Corp. and the Preliminary Examination Instructions

- Following the *Alice Corp.* decision, the USPTO issued “Preliminary Examination Instructions” in a memorandum to the examining corps on June 25, 2014.
  - Accessible at www.USPTO.gov at the webpage titled: “Examination Guidance and Training Materials”

- Public comments on the *Alice Corp.* Preliminary Examination Instructions were invited for 30 days.
  - 79 Fed. Reg. 38854 (June 30, 2014)
  - 47 Comments were received and can be viewed on the website at the webpage titled: “Comments from the Public”
• *Alice Corp.* requires several changes in USPTO practice because prior examination guidance:
  – Applied a different analysis to claims with abstract ideas than to claims with laws of nature.
  – Applied a different analysis to product claims involving abstract ideas than to process claims.

• The Preliminary Examination Instructions were issued to immediately address abstract ideas.
  – Laws of nature and natural phenomena are already being analyzed under *Mayo.*
Analyzing Claims with Abstract Ideas: Basic Inquiries

The basic inquiries to determine subject matter eligibility under 35 USC 101 remain the same (MPEP 2106(I)):

• First, determine whether the claim is directed to one of the four statutory categories of invention, *i.e.*, process, machine, manufacture, or composition of matter.
  – If not, the claim is ineligible because it is directed to non-statutory subject matter. (*e.g.*, information *per se*.)

• Next, determine whether the claim is directed to a judicial exception and, if so, whether it is directed to a patent-eligible application of the exception.
  • Under *Alice Corp.* this is a two-part analysis.
Two-part Analysis for Abstract Ideas

• **Part 1:** Determine whether the claim is directed to an abstract idea (a judicial exception).
  – If not, the claim is eligible. If so, proceed to Part 2.

• **Part 2:** Determine whether any element, or combination of elements, in the claim is sufficient to ensure that the claim as a whole amounts to **significantly more** than the abstract idea itself.
  – If so, the claim is eligible. If not, the claim is ineligible because it is directed to non-statutory subject matter.
Part 1: Is the claim directed to an abstract idea?

- It is important to remember that at some level, all inventions embody, use, reflect, rest upon or apply abstract ideas and the other exceptions.
  - An invention is not ineligible simply because it involves an abstract concept.

- Examples of abstract ideas referenced in *Alice Corp.* include:
  - Fundamental economic practices;
  - Certain methods of organizing human activities;
  - “[A]n idea of itself”; and,
  - Mathematical relationships/formulas.
Part 2: Does any element, or combination of elements, amount to significantly more than the abstract idea itself?

- In other words, are there other limitations in the claim that show a patent-eligible application of the abstract idea, e.g., more than a mere instruction to apply the abstract idea?

- Analyze the claim as a whole.
• Limitations referenced in *Alice Corp.* that may be enough to qualify as “significantly more” when recited in a claim with an abstract idea:

- Improvements to another technology or technical field.
- Improvements to the functioning of the computer itself.
- Meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment.
Limitations referenced in *Alice Corp.* that are **not** enough to qualify as “significantly more” when recited in a claim with an abstract idea:

- Adding the words “apply it” (or an equivalent) with an abstract idea.
- Mere instructions to implement an abstract idea on a computer.
- Requiring no more than a generic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry.
A number of comments supported the preliminary guidance, including that the instructions:

- accurately reflect the *Alice* decision.
- correctly state that there is no *per se* excluded category of subject matter.
- correctly state that claims should be treated as a whole.
A number of comments proposed modifications to the guidance, including that:

- “significantly more” inquiry should focus on preemption and/or an “inventive concept.”
- final guidelines should be more detailed and/or should provide examples.
- “directed to” should be clarified and used consistently.
Public Comments on Preliminary Examination Instructions

• Some comments expressed a desire for more reasoned explanation in Office actions.

• There were mixed opinions on the impact of *Alice Corp.* with respect to what should be considered as an abstract idea.

• There were mixed opinions on whether future guidance examples should be limited to judicial precedent or expanded to other subject matter.

• A number of comments included specific proposed claim examples, examples of “abstract ideas,” guiding cases, and/or proposed changes to the language of the Instructions.
Next Steps: New Guidance

• Next iteration of guidance is now being developed and should issue soon.
  • Following the approach taken by the Supreme Court in *Alice Corp.*, the guidance is planned to address process and product claims directed to a judicial exception.
  • It is anticipated that there will be supplements with additional information and examples.
  • Public comments were considered in drafting this iteration and will be used in developing examples.
• The next iteration of guidance will again solicit comments from the public for further refinements in examination procedure.
• Federal Circuit decisions will be closely watched for further developments.
Cybersecurity Partnership Meeting

The USPTO will host its first industry partnership meeting with the cybersecurity and network security community in California Friday, November 14, 2014.
Thank You
Q&A
Break
David Kinsinger
Vice President, Chief Patent Counsel, L-3

United States Patent and Trademark Office
November 14, 2014 in Menlo Park, CA
Effective Cybersecurity: Protecting Your Intellectual Property Assets

Cybersecurity Partnership
November 14, 2014
Silicon Valley USPTO
Think of a city somewhere unexpected that you have visited or would like to someday visit.
Need for Cybersecurity

“Cyber threat is one of the most serious economic and national security challenges we face as a nation.”

“America's economic prosperity in the 21st century will depend on cybersecurity.”

—President Barrack Obama
The Value of Information

- In 1978, 83% of a firm’s value was associated with tangible assets, with 17% associated with intangible.
- By 1998, only 31% of the firm’s value was associated with tangible assets, with 69% associated with the value of their intangibles.
- 2014?

- Source: Edison in The Boardroom
  Authors: Julie Davis and Suzanne Harrison
Hope and Change

- How vulnerable are you to attack?
- Can I steal your data?
- Think of a number from 1 to 100.
- Could I possibly know what you are thinking?
- When did I know it?
An internet-borne attack usually perpetrated by a group of individuals with significant resources, such as organized crime or a rogue nation-state.

“Emerging cyber tactics are designed to evade traditional cyber defenses and escape detection until it’s too late.”
Malware

Malicious software or code that typically damages or disables, takes control of, or steals information from a computer system. Broadly includes viruses, worms, Trojan horses, logic bombs, rootkits, bootkits, backdoors, spyware, and adware.
A Weapon

- Think of a weapon, but make it something unusual or unexpected.
Cybersecurity Market

- $95 Billion in 2014
- $155 Billion by 2019
- Market Types:
  - Network Security; Endpoint Security; Application Security; Content Security; Wireless Security; Cloud Security
- Solutions:
  - Identity and access management; risk and compliance management; encryption; data loss protection; unified threat management; firewall; anti-virus; anti-malware
In 2013, Cybercrime cost businesses an estimated $575 billion.

“Evidence suggests a gap between the magnitude of exposure presented by cyber-risks and the steps, or lack thereof, that many corporate board have taken to address these risks.”

– SEC Commissioner Luis Aguilar

NYSE security filings using the words “cybersecurity”, “hacking”, “hackers”, “cyberattacks”, or “data breach”:

- 2012 – 879 firms
- 2013 – 1,288 firms
- 2014 – 1,517 firms
Mobile Computing

- Need to balance user security and convenience.
- Customers want convenience.
- Mobile environment is particularly vulnerable.
- “Mobile malware is winning.”
- Must approach solutions in a comprehensive, risk-based manner.
Insider Threats

- Edward Snowden
- Compartmentalization of critical information
- Data exfiltration prevention solutions
- Automated solutions to identify suspect behavior of insiders – advanced analytics
- Identity management
- User authentication
  - Biometric solutions
- Role-based access techniques
- “With Wi-Fi and high capacity jump drives, anybody can walk out of a room with 65 gigabytes of info on her keychain.”
The Internet

- “The internet is the guy with the gun.”
- “If it touches the internet, it can be taken.”
- “The only way to be safe is to remove yourself from the internet.”
How do you get the attention of a room full of attorneys?

It helps to know how you think.
Comprehensive I.P. Protection

- Trade Secrets
- Patent Portfolio
- Defensive Publishing
- Enabled Documentation
- IP Insurance
  - Cyber Insurance
Question: Patent or Trade Secret?
Simple Answer: Both!
- Adherence to Best Mode Requirement
- Cyber Threats may shift the balance
A famous person

- Think of a famous person... someone that I would know, but that I would not expect.
“The first thing you want in a new country is a patent office.”
–Mark Twain, 1889
Enables threat information from multiple sensors to be combined and shared across organizations
Coordinates a distributed defense strategy in response to designated threats
Pushes the defense as close as possible to the sources of the threats
Fast, Efficient, Scalable, Collaborative
Assignee: Phillips Petroleum Company

We claim:

1. Normally solid polypropylene, consisting essentially of recurring polypropylene units, having a substantial crystalline polypropylene content.
We claim:
1. A method of managing undesirable network traffic transmitted from a source node to a destination node over a communications network, comprising:
   receiving, by a computing device, a first notification of a routing rule change for the destination node;
   determining, by a computing device, a first network entity corresponding to the destination node and indicated by the first notification;
   determining, based on the first network entity, an identifier;
   determining, by a computing device, a network address of a node maintaining network routing rules for the first network entity and the destination node based on the identifier and public data;
   querying, by a computing device, the node maintaining network routing rules for one or more routing rules based on the network address;
   receiving a response to the query from the node maintaining network routing rules;
   determining, via a computing device, one or more network routing rules based on the response to the query;
   applying at least one of the determined one or more network routing rules to at least one network device;
   determining a network path toward the source node;
   determining a network address for a device managed by a second network entity, different than the first network entity, based on the network path;
   determining the second network entity based on the network path and the network address of the device managed by the second network entity;
   determining, based on the second network entity, a second identifier;
   determining a node maintaining network routing rules for the second network entity based on the second identifier and public data; and
   transmitting, by a computing device, a second notification of the routing rule change to the node maintaining network routing rules for the second network entity over the communications network.
New authentication approaches will replace password

- Fingerprint
- Voice Recognition
- Facial Recognition
- Combined Approaches
  - Biometrics
  - Encryptic PIN’s
  - Secure Device Provisioning
4–D Telepathy

- Are your passwords protected and safe?
- If I can steal your password in a few minutes, what can the cybercriminal do?
The Law Firm as a Target

- ABA Model Rules of Professional Conduct: “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information, relating to the representation of a client.”
- Protecting confidential client data is becoming more difficult.
- Survey: 89% of law 300 legal professionals said their firms send confidential information to clients via unencrypted email.
- Law firms have big bull’s-eye status because they are viewed as vulnerable and are known to maintain material that hackers would consider to be of high value.
Proactive approach

- Assume you are a target
- Involve executive management
- Map and encrypt data
- Seek comprehensive security solutions from firewalls to antivirus programs to multilayers of defensive technology
- Train employees to understand cyber risks
- Plan for the worst
- Have a trained response team ready when a breach occurs
Cyber Insurance

- Standard insurance policies are not designed to address losses from data breaches.
- Businesses should consider specialty cyber policies for protection against data theft or loss.
- Factors to consider:
  - Damages or expenses covered
  - Type of information loss covered
  - Application to third-party vendors
  - Requirements for breach during specified periods
  - Requirements to maintain and update computer systems
- Policies should be tailored to match your cyber risks.
NIST Cyber Framework

- Voluntary risk-based compilation of guidelines that aims to help organizations identify, implement, and improve their cybersecurity stance
- Useful for communicating risk management by establishment of a detection baseline and aggregating and correlating the event data
NIST Framework Core

- Organized by five continuous functions:
  - **Identify**: managing cybersecurity risks to systems, assets, data and capabilities
  - **Protect**: controls and safeguards to protect assets or deter threats
  - **Detect**: continuous monitoring for proactive real-time alerts of cybersecurity events
  - **Respond**: policies and activities necessary for prompt responses to cybersecurity incidents
  - **Recover**: business continuity plans to recover capabilities after a breach
Companies should adopt the guidelines as a tool to manage and mitigate cyber risk in combination with other risk-management tools and processes including cyber insurance.

Four Steps
1. Identify your executive business sponsor and engage
2. Assess your current posture
3. Define a target profile and execute
4. Continuously monitor, communicate, and collaborate
1. Use the NIST framework as Guidance
2. Institute broad structural changes to focus on appropriate Cyber-Risk Management
3. Maintain appropriate personnel
4. Be prepared!
Protect your IP Assets

- Be innovative, then protect your innovation.
- Be proactive not reactive.
- Be prepared to act.
- The game of Clue: Who, how, where?
Sec. 112(b): Nautilus
...Packard ... Miyazaki

Cybersecurity Partnership
November 14, 2014; Silicon Valley USPTO, Menlo Park, California
John D. Vandenberg
Nautilus: Impact?

- **Phrasing:** “clarity and precision demand;” “clear notice;” “reasonable certainty”

- **Unambiguous:** Prohibits ambiguity

- **Not Post Hoc:** Rejects *post hoc*, claim-construction-first, hindsight approach
  
o. Do **not** first construe claim and then ask whether crystal ball showing that construction would have provided sufficient notice to artisan.

- **How Precise?:** Not “absolute precision,” but must claim be as precise as the subject matter permits?
In re Packard, 751 F.3d 1307(Fed. Cir. 2014): “when the USPTO has initially issued a well-grounded rejection that identifies ways in which language in a claim is ambiguous, vague, incoherent, opaque, or otherwise unclear in describing and defining the claimed invention, and thereafter the applicant fails to provide a satisfactory response, the USPTO can properly reject the claim as failing to meet the statutory requirements of § 112(b).”

S. Ct.: (1) Presumption of validity does not alter degree of clarity demanded; (2) Eliminating temptation to inject ambiguity “is in order;” (3) Not deciding: “whether deference is due to the PTO’s resolution of disputed issues of fact.”
No Genuine Ambiguity: “we hold that if a claim is amenable to two or more plausible claim constructions, the USPTO is justified in” rejecting the claim as indefinite.

No Purely Functional Elements: A claim may not contain a “purely functional claim element with no limitation of structure” in the claim (expressly or under Sec. 112, ¶ 6), whether or not at the point of novelty.

*Ex Parte Miyazaki,*

89 USPQ2d 1207 (BPAI 2008) (precedential)
Recommendation 1

- USPTO: Enforce second holding of *Ex Parte Miyazaki* by prohibiting “purely functional” limitations. Encourage Sec. 112(f) elements:
  - Statutory safe haven from Sec. 112(b) if truly satisfy Sec. 112(f)
  - More likely to survive Sec. 101 challenge too ... if disclosed “structure” is in the physical realm
Recommendation 2

- USPTO and Applicants: Do not treat a result as a function:
  - Sec. 112(f): “a means or step for performing a specified function”
  - Doctrine of Equivalents: “if it performs substantially the same function in substantially the same way to obtain the same result.”
- Especially important to prohibit “result” claiming.
Recommendation 3

➤ **USPTO**: Break applicants’ bad (ambiguity) habits:
  - Preambles that *maybe* are limitations
  - Language that *maybe* triggers Sec. 112(f)
  - Terms that *maybe* are functional.
Recommendation 4

- **USPTO and Applicants**: Do not conflate enablement with particular and distinct claiming:
  - **Enablement**: Can artisan who wants to practice claimed invention do so?
  - **Particular and Distinct Claiming**: Can artisan who wants to avoid claimed invention and innovate just outside its boundary, see that boundary with reasonable certainty?
Recommendation 5

➢ USPTO: Apply Sec. 101 law hand-in-hand with Sec. 112(b) law:
  o “Abstract” \(\approx\) not “Particular”
  o Limit preemptive footprint to balance needs of applicant-inventor vs. would-be-next-inventor
Nautilus: Old Design ... Better Result

Live electrode

“Spaced Relationship”

Common electrode
1. A heart rate monitor for use by a user in association with exercise apparatus and/or exercise procedures, comprising; an elongate member;

a first live electrode and a first common electrode mounted on said first half in spaced relationship with each other;
a second live electrode and a second common electrode mounted on said second half in spaced relationship with each other;

whereby, a first electromyogram signal will be detected between said first live electrode and said first common electrode, and a second electromyogram signal, of substantially equal magnitude and phase to said first electromyogram signal will be detected between said second live electrode and said second common electrode;
If “spaced relationship” is itself functional, then:
  o Artisans could safely explore different techniques (e.g., new materials) for achieving claimed result with this old design.

But if “spaced relationship” is not functional, then:
  o No way of achieving claimed result with this old design would be safe.
Q&A
Break
Open Panel Discussion

Moderator: John Cabeca
Panelists: Angela Ziegenhorn, David Kinsinger, John Vandenberg, Kevin Stine, Michael Cygan, Nestor Ramirez
Overview of Examiner Training on Functional Claiming

Michael Cygan
Senior Legal Advisor
Office of Patent Legal Administration
Recently Completed Examiner Training

• Four examiner training modules (one hour each):
  o **Module 1**: Identifying § 112(f) limitations
    ▪ Recognizing § 112(f) limitations that do not use classic “means for” phrasing
    ▪ Interpreting “generic placeholders” that serve as substitutes for means (e.g., unit, mechanism)
  o **Module 2**: Clarifying the record to place remarks in the file regarding when § 112(f) is, or is not, invoked
    ▪ Establishing presumptions based on use of “means”
    ▪ Providing explanatory remarks when presumptions are rebutted
Recently Completed Examiner Training

• **Module 3**: Interpretation and definiteness of 35 U.S.C. § 112(f) limitations
  o How to interpret § 112(f) limitations under the broadest reasonable interpretation (BRI) standard
  o Evaluating equivalents
  o Determining whether a § 112(f) limitation is definite under § 112(b)

• **Module 4**: Computer-implemented (software) § 112(f) limitations
  o Determining whether a sufficient algorithm is provided to support a software function
Panel Topic:
Examination Best Practices and Ways to Advance Prosecution
Panel Topic:
Stakeholder perspectives and Identifying topics for future partnership meetings
Closing Remarks

John Cabeca, Director, Silicon Valley USPTO
Thank You

United States Patent and Trademark Office
November 14, 2014 in Menlo Park, CA