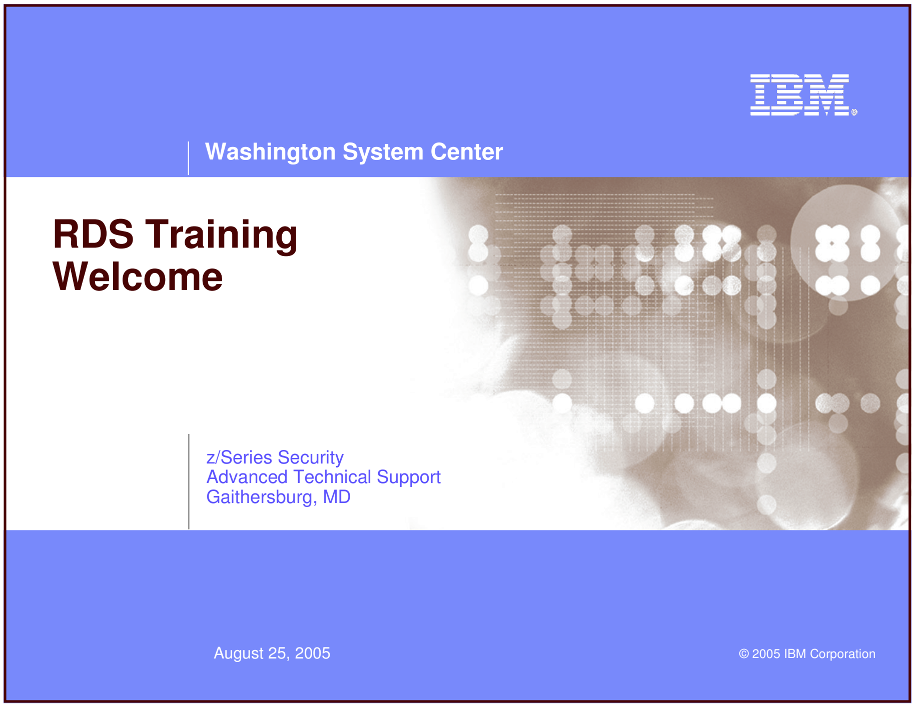
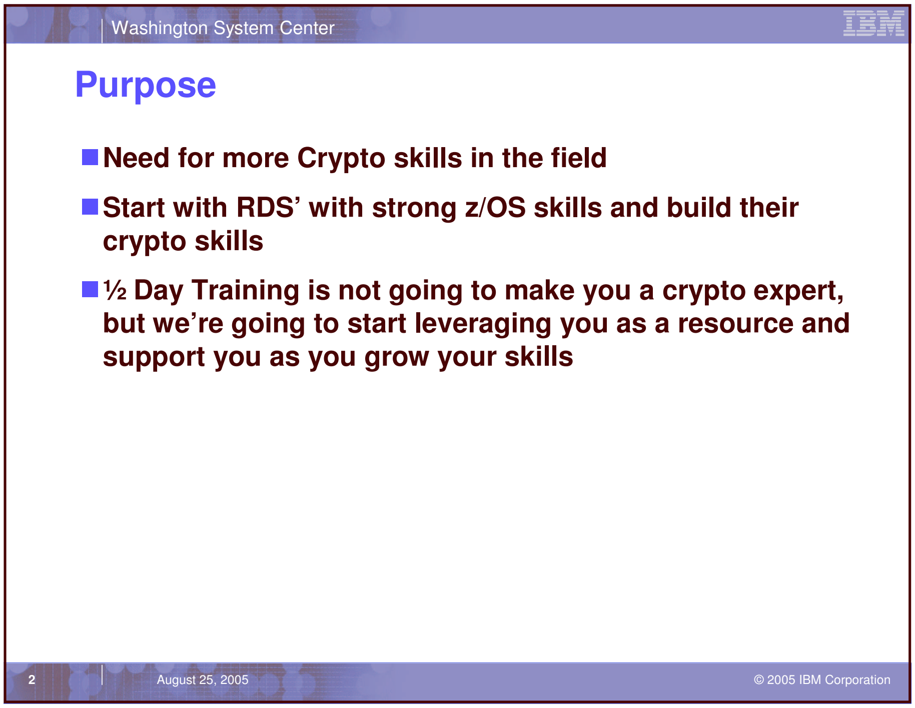


Washington System Center

# RDS Training Welcome

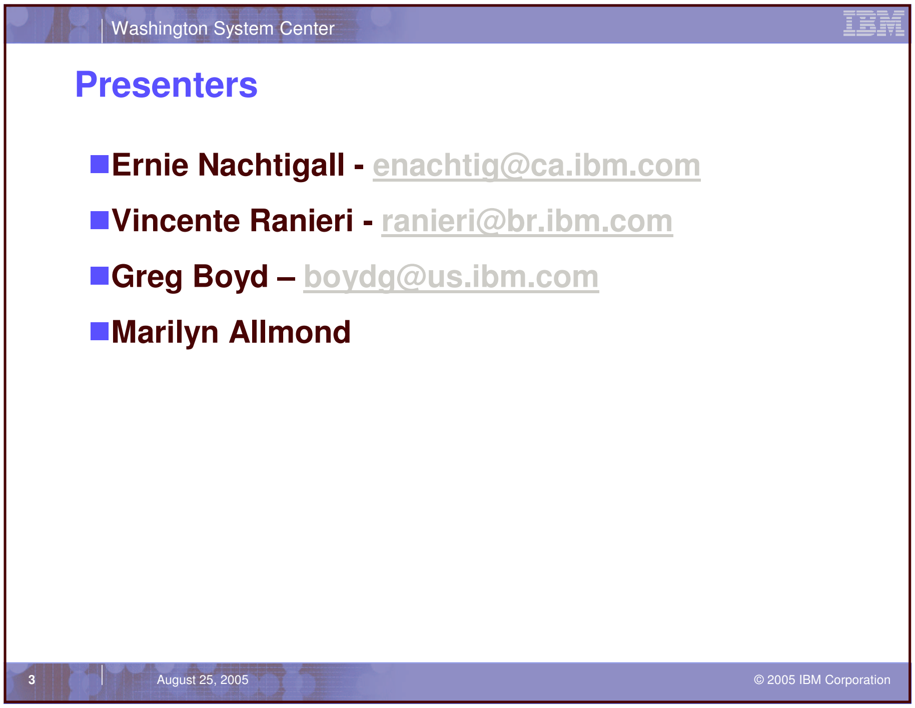
z/Series Security
Advanced Technical Support
Gaithersburg, MD

August 25, 2005



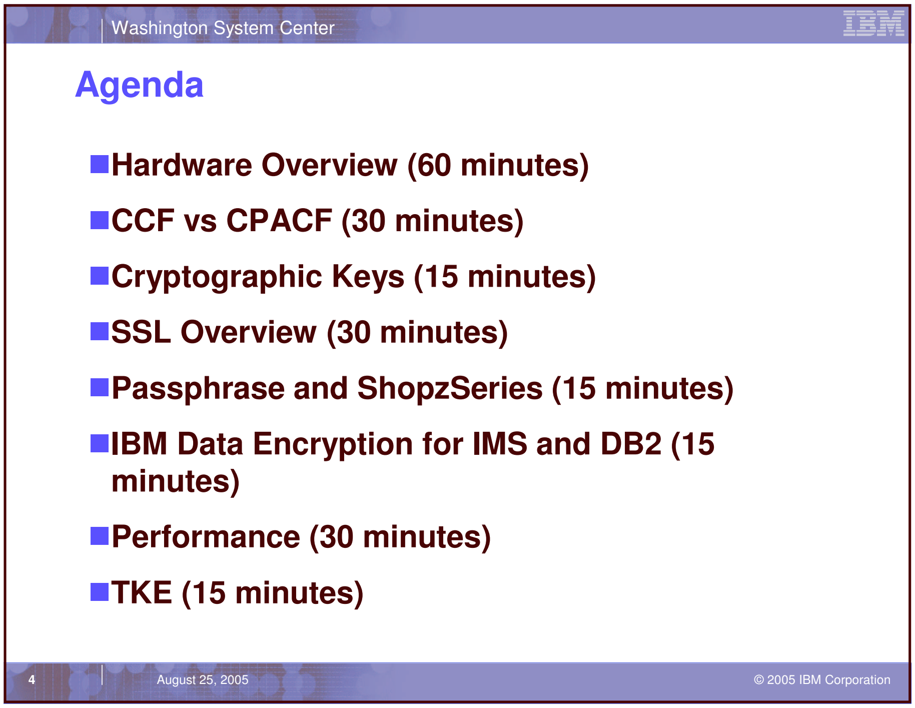
## Purpose

- Need for more Crypto skills in the field
- Start with RDS’ with strong z/OS skills and build their crypto skills
- ½ Day Training is not going to make you a crypto expert, but we’re going to start leveraging you as a resource and support you as you grow your skills



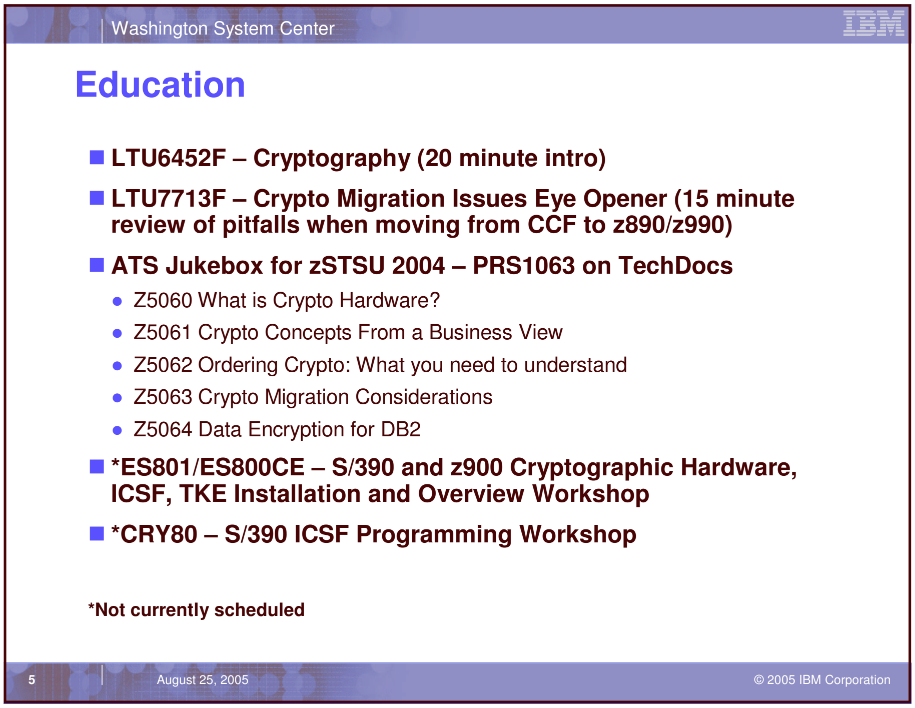
## Presenters

- Ernie Nachtigall - enachtig@ca.ibm.com
- Vincente Ranieri - ranieri@br.ibm.com
- Greg Boyd – boydg@us.ibm.com
- Marilyn Allmond



## Agenda

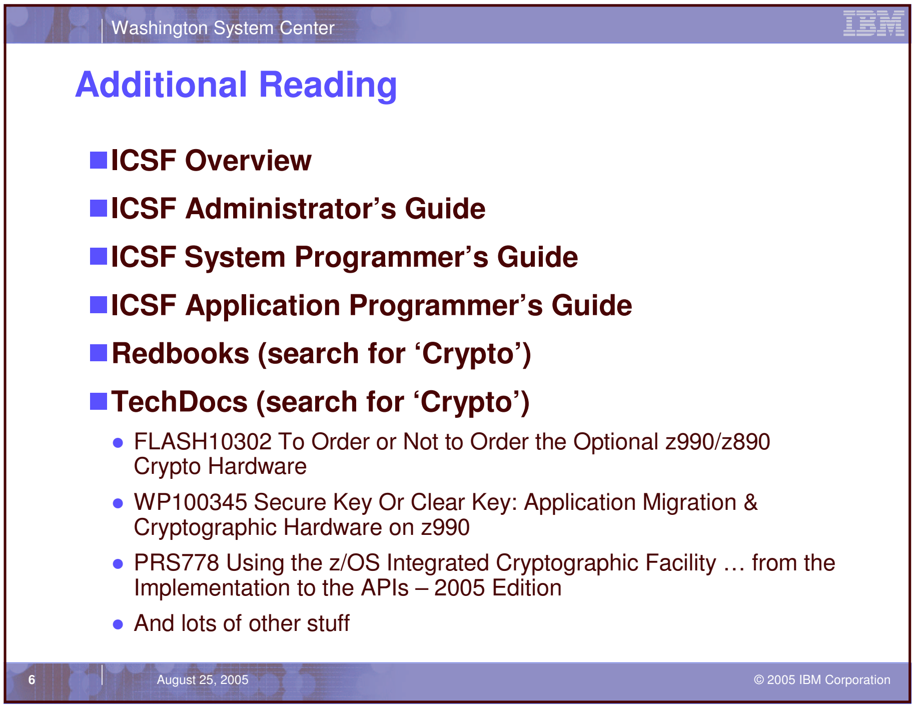
- Hardware Overview (60 minutes)
- CCF vs CPACF (30 minutes)
- Cryptographic Keys (15 minutes)
- SSL Overview (30 minutes)
- Passphrase and ShopzSeries (15 minutes)
- IBM Data Encryption for IMS and DB2 (15 minutes)
- Performance (30 minutes)
- TKE (15 minutes)



## Education

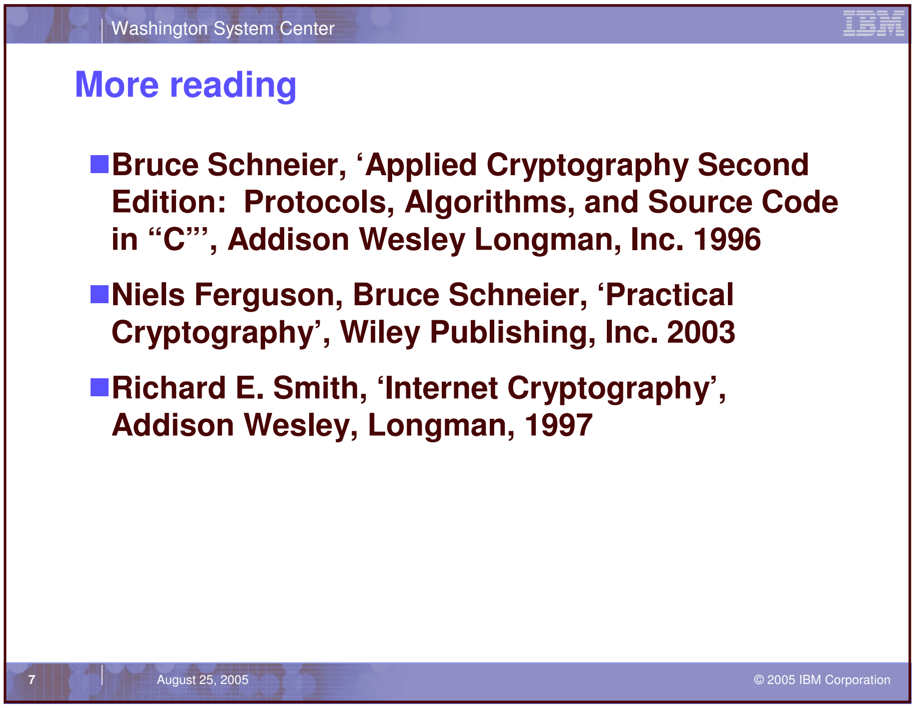
- **LTU6452F – Cryptography (20 minute intro)**
- **LTU7713F – Crypto Migration Issues Eye Opener (15 minute review of pitfalls when moving from CCF to z890/z990)**
- **ATS Jukebox for zSTSU 2004 – PRS1063 on TechDocs**
  - Z5060 What is Crypto Hardware?
  - Z5061 Crypto Concepts From a Business View
  - Z5062 Ordering Crypto: What you need to understand
  - Z5063 Crypto Migration Considerations
  - Z5064 Data Encryption for DB2
- ***ES801/ES800CE – S/390 and z900 Cryptographic Hardware, ICSF, TKE Installation and Overview Workshop**
- ***CRY80 – S/390 ICSF Programming Workshop**

***Not currently scheduled**



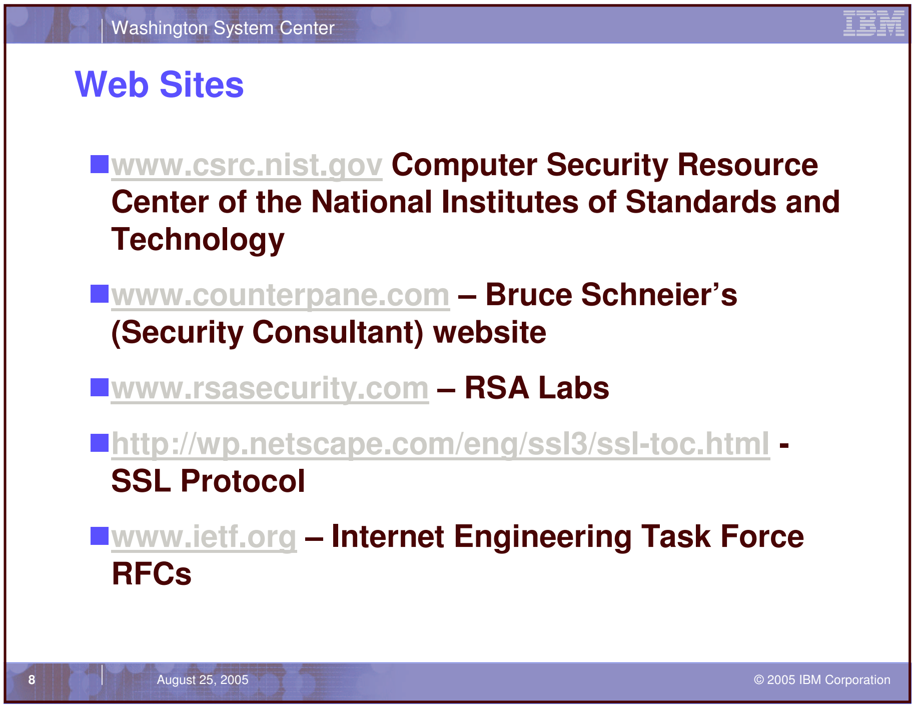
## Additional Reading

- **ICSF Overview**
- **ICSF Administrator’s Guide**
- **ICSF System Programmer’s Guide**
- **ICSF Application Programmer’s Guide**
- **Redbooks (search for ‘Crypto’)**
- **TechDocs (search for ‘Crypto’)**
  - FLASH10302 To Order or Not to Order the Optional z990/z890 Crypto Hardware
  - WP100345 Secure Key Or Clear Key: Application Migration & Cryptographic Hardware on z990
  - PRS778 Using the z/OS Integrated Cryptographic Facility … from the Implementation to the APIs – 2005 Edition
  - And lots of other stuff



## More reading

- Bruce Schneier, ‘Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in “C”’, Addison Wesley Longman, Inc. 1996
- Niels Ferguson, Bruce Schneier, ‘Practical Cryptography’, Wiley Publishing, Inc. 2003
- Richard E. Smith, ‘Internet Cryptography’, Addison Wesley, Longman, 1997



## Web Sites

- www.csrc.nist.gov Computer Security Resource Center of the National Institutes of Standards and Technology
- www.counterpane.com – Bruce Schneier’s (Security Consultant) website
- www.rsasecurity.com – RSA Labs
- http://wp.netscape.com/eng/ssl3/ssl-toc.html - SSL Protocol
- www.ietf.org – Internet Engineering Task Force RFCs