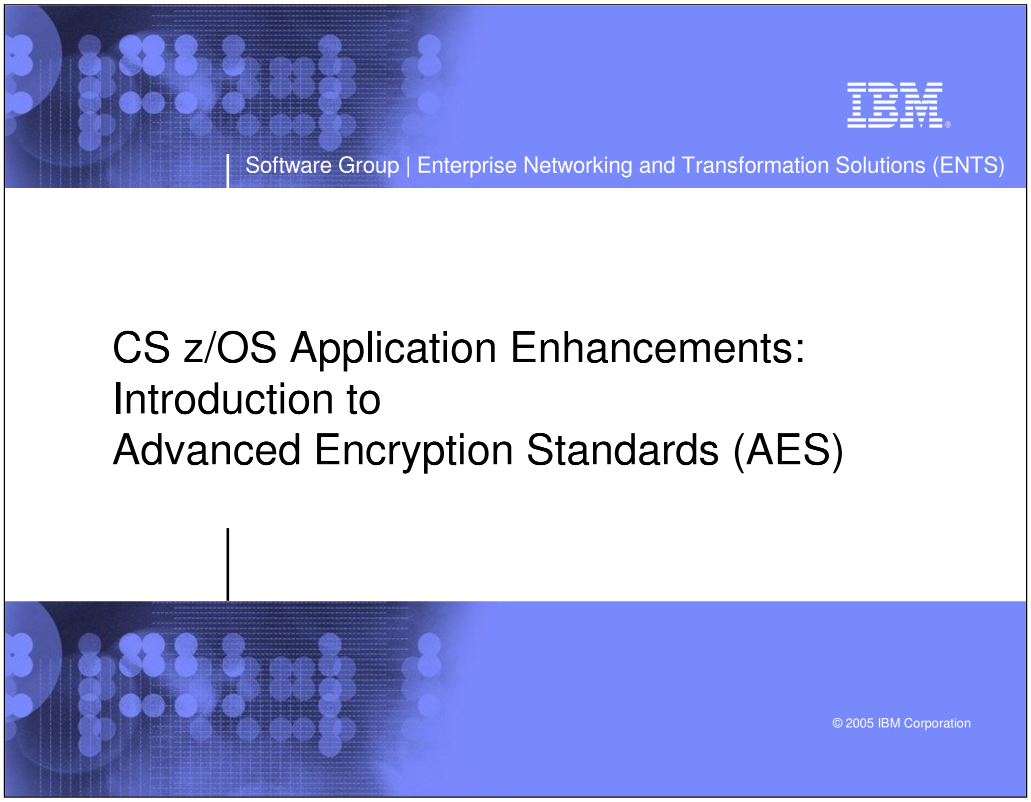
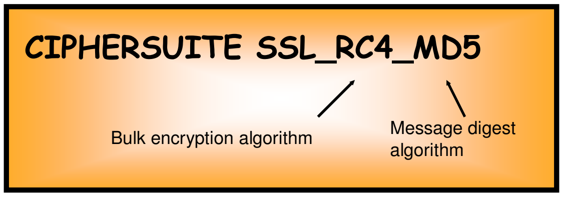


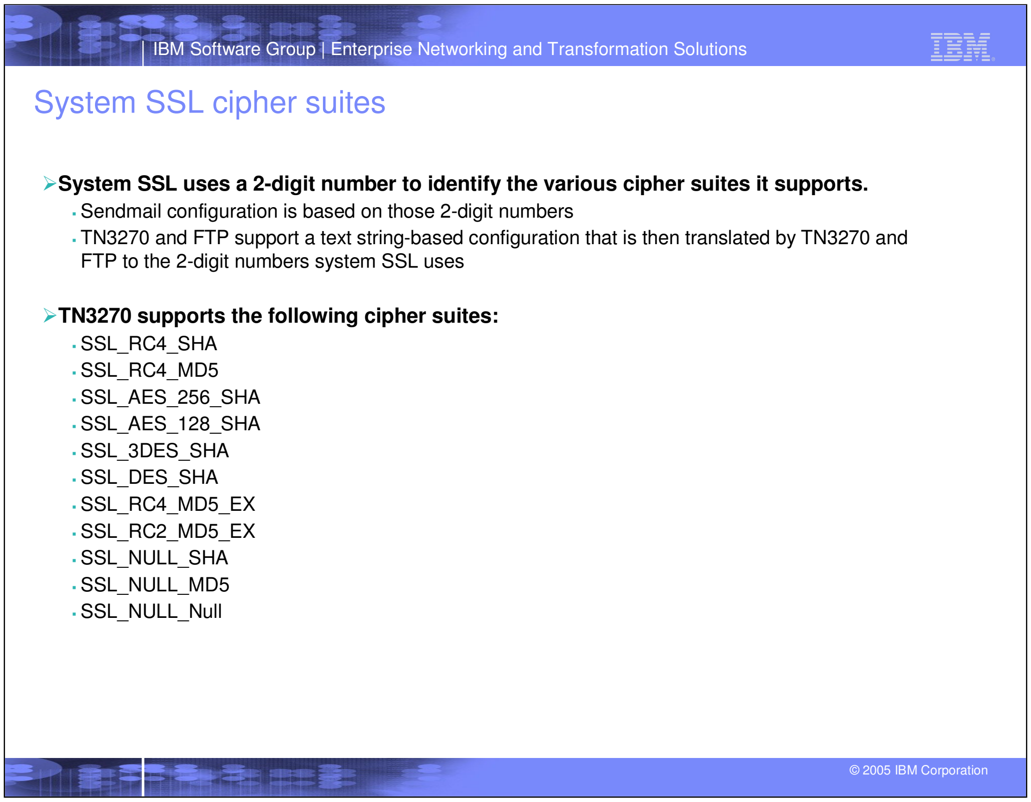
CS z/OS Application Enhancements: Introduction to Advanced Encryption Standards (AES)

A little background information on cipher suites

A cipher suite is of a collection of cryptographic algorithms:

- A key exchange algorithm
  - System SSL on z/OS uses RSA algorithms for key exchange - also known as public private key or assymetric encryption
  - Authentication is based on digital x.509 certificates
  - SSL/TLS server always has a certificate; SSL/TLS client may optionally have a certificate also
- A bulk encryption algorithm
  - Used to encrypt/decrypt the data that is exchanged between the connection endpoints
  - Needs to be fast and efficient - symmetric encryption algorithms are used for this purpose
- A message digest algorithm
  - Used to ensure each message exchange has not been altered in transit, and that it came from the intended sender (also sometimes referred to as a digital signature)





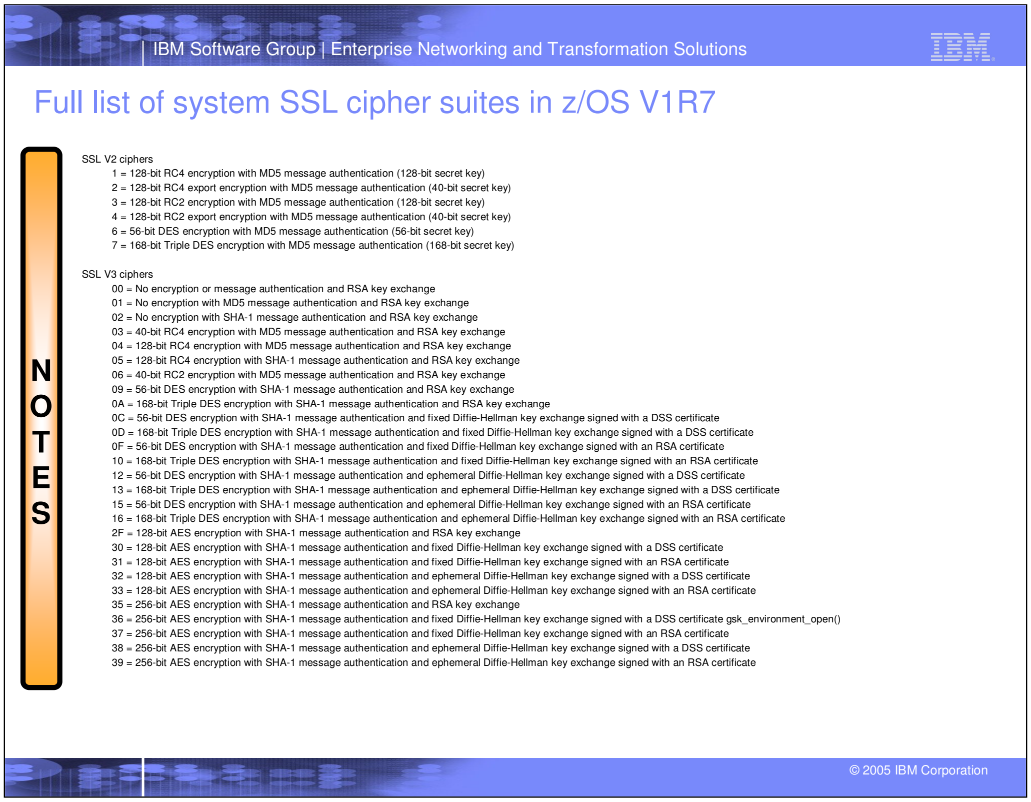
System SSL cipher suites

- **System SSL uses a 2-digit number to identify the various cipher suites it supports.**
  - Sendmail configuration is based on those 2-digit numbers
  - TN3270 and FTP support a text string-based configuration that is then translated by TN3270 and FTP to the 2-digit numbers system SSL uses

- **TN3270 supports the following cipher suites:**
  - SSL_RC4_SHA
  - SSL_RC4_MD5
  - SSL_AES_256_SHA
  - SSL_AES_128_SHA
  - SSL_3DES_SHA
  - SSL_DES_SHA
  - SSL_RC4_MD5_EX
  - SSL_RC2_MD5_EX
  - SSL_NULL_SHA
  - SSL_NULL_MD5
  - SSL_NULL_Null

System SSL cipher suites *(continued)*

- **FTP supports the following cipher suites:**
  - SSL_DES_SHA
  - SSL_3DES_SHA
  - SSL_NULL_MD5
  - SSL_NULL_SHA
  - SSL_RC2_MD5_EX
  - SSL_RC4_MD5
  - SSL_RC4_MD5_EX
  - SSL_AES_128_SHA
  - SSL_AES_256_SHA



Full list of system SSL cipher suites in z/OS V1R7

NOTES

SSL V2 ciphers

1 = 128-bit RC4 encryption with MD5 message authentication (128-bit secret key)

2 = 128-bit RC4 export encryption with MD5 message authentication (40-bit secret key)

3 = 128-bit RC2 encryption with MD5 message authentication (128-bit secret key)

4 = 128-bit RC2 export encryption with MD5 message authentication (40-bit secret key)

6 = 56-bit DES encryption with MD5 message authentication (56-bit secret key)

7 = 168-bit Triple DES encryption with MD5 message authentication (168-bit secret key)

SSL V3 ciphers

00 = No encryption or message authentication and RSA key exchange

01 = No encryption with MD5 message authentication and RSA key exchange

02 = No encryption with SHA-1 message authentication and RSA key exchange

03 = 40-bit RC4 encryption with MD5 message authentication and RSA key exchange

04 = 128-bit RC4 encryption with MD5 message authentication and RSA key exchange

05 = 128-bit RC4 encryption with SHA-1 message authentication and RSA key exchange

06 = 40-bit RC2 encryption with MD5 message authentication and RSA key exchange

09 = 56-bit DES encryption with SHA-1 message authentication and RSA key exchange

0A = 168-bit Triple DES encryption with SHA-1 message authentication and RSA key exchange

0C = 56-bit DES encryption with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with a DSS certificate

0D = 168-bit Triple DES encryption with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with a DSS certificate

0F = 56-bit DES encryption with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with an RSA certificate

10 = 168-bit Triple DES encryption with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with an RSA certificate

12 = 56-bit DES encryption with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with a DSS certificate

13 = 168-bit Triple DES encryption with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with a DSS certificate

15 = 56-bit DES encryption with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate

16 = 168-bit Triple DES encryption with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate

2F = 128-bit AES encryption with SHA-1 message authentication and RSA key exchange

30 = 128-bit AES encryption with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with a DSS certificate

31 = 128-bit AES encryption with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with an RSA certificate

32 = 128-bit AES encryption with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with a DSS certificate

33 = 128-bit AES encryption with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate

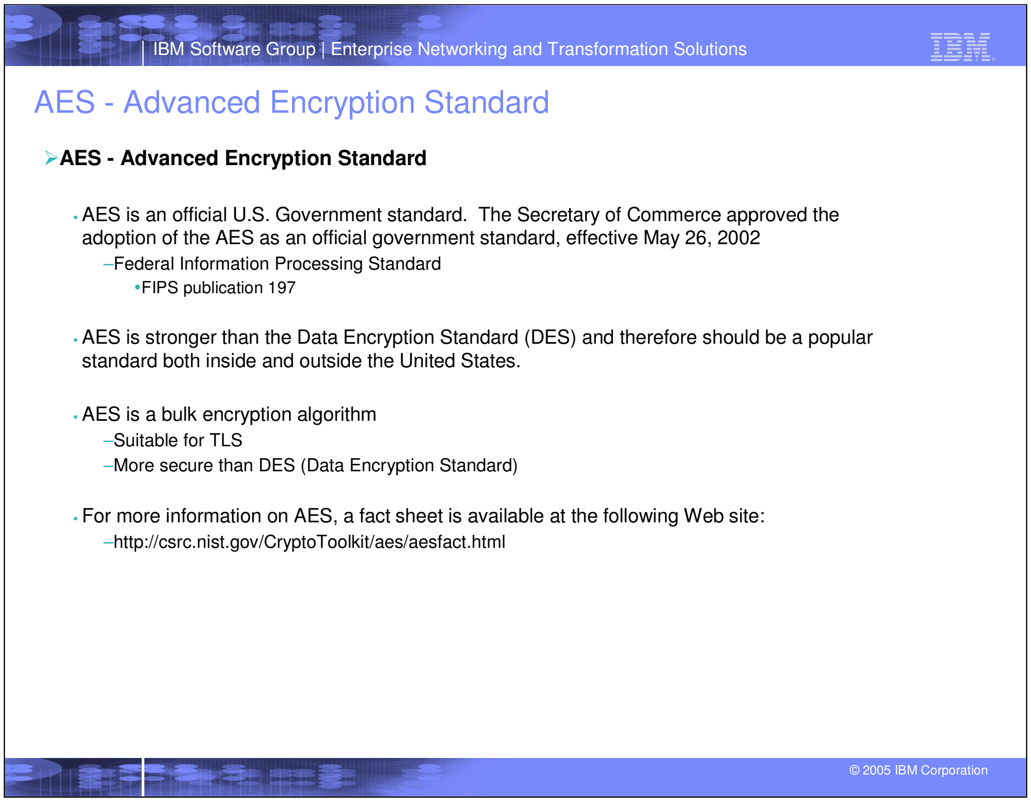
35 = 256-bit AES encryption with SHA-1 message authentication and RSA key exchange

36 = 256-bit AES encryption with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with a DSS certificate gsk_environment_open()

37 = 256-bit AES encryption with SHA-1 message authentication and fixed Diffie-Hellman key exchange signed with an RSA certificate

38 = 256-bit AES encryption with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with a DSS certificate

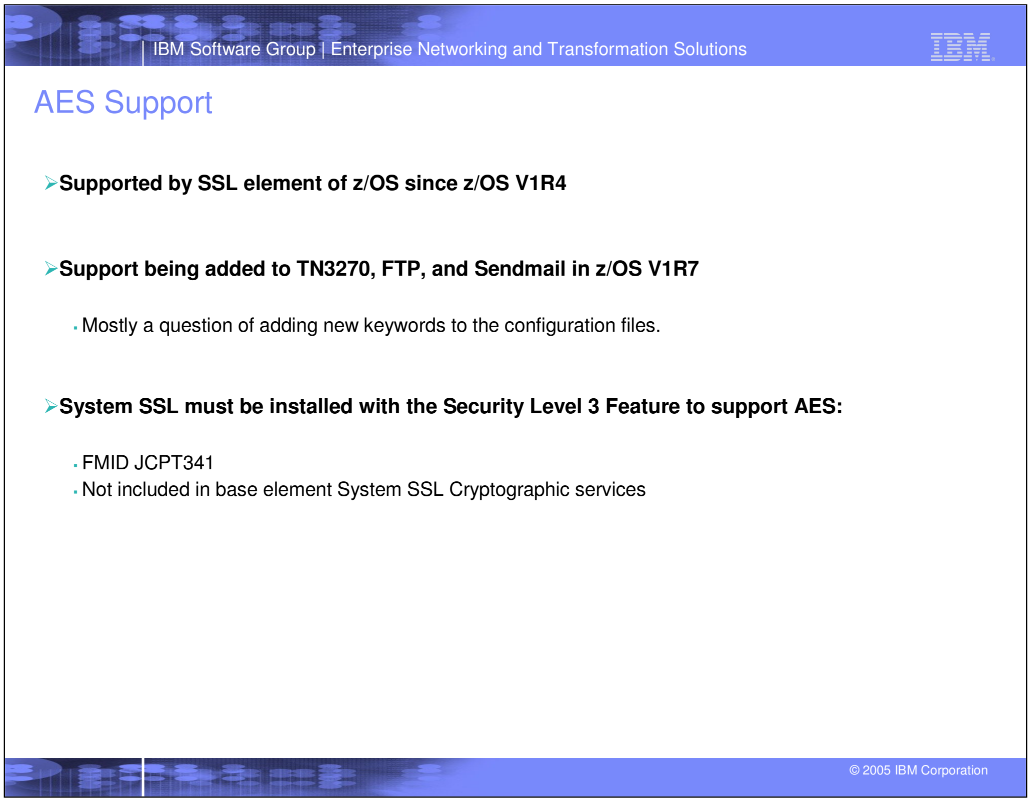
39 = 256-bit AES encryption with SHA-1 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate



AES - Advanced Encryption Standard

➢AES - Advanced Encryption Standard

- AES is an official U.S. Government standard. The Secretary of Commerce approved the adoption of the AES as an official government standard, effective May 26, 2002
  - Federal Information Processing Standard
    - FIPS publication 197
- AES is stronger than the Data Encryption Standard (DES) and therefore should be a popular standard both inside and outside the United States.
- AES is a bulk encryption algorithm
  - Suitable for TLS
  - More secure than DES (Data Encryption Standard)
- For more information on AES, a fact sheet is available at the following Web site:
  - http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html

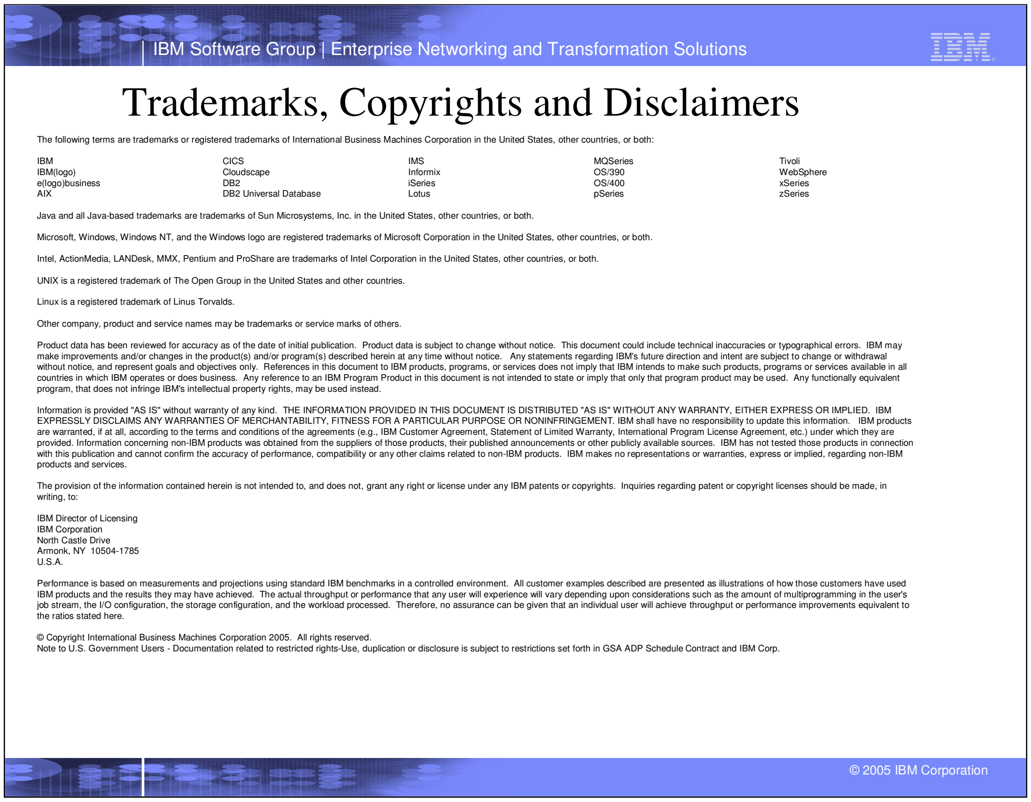


AES Support

- **Supported by SSL element of z/OS since z/OS V1R4**

- **Support being added to TN3270, FTP, and Sendmail in z/OS V1R7**
  - Mostly a question of adding new keywords to the configuration files.

- **System SSL must be installed with the Security Level 3 Feature to support AES:**
  - FMID JCPT341
  - Not included in base element System SSL Cryptographic services



Trademarks, Copyrights and Disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
IBM(logo)
e(logo)business
AIX
CICS
Cloudscape
DB2
DB2 Universal Database
IMS
Informix
iSeries
Lotus
MQSeries
OS/390
OS/400
pSeries
Tivoli
WebSphere
xSeries
zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.