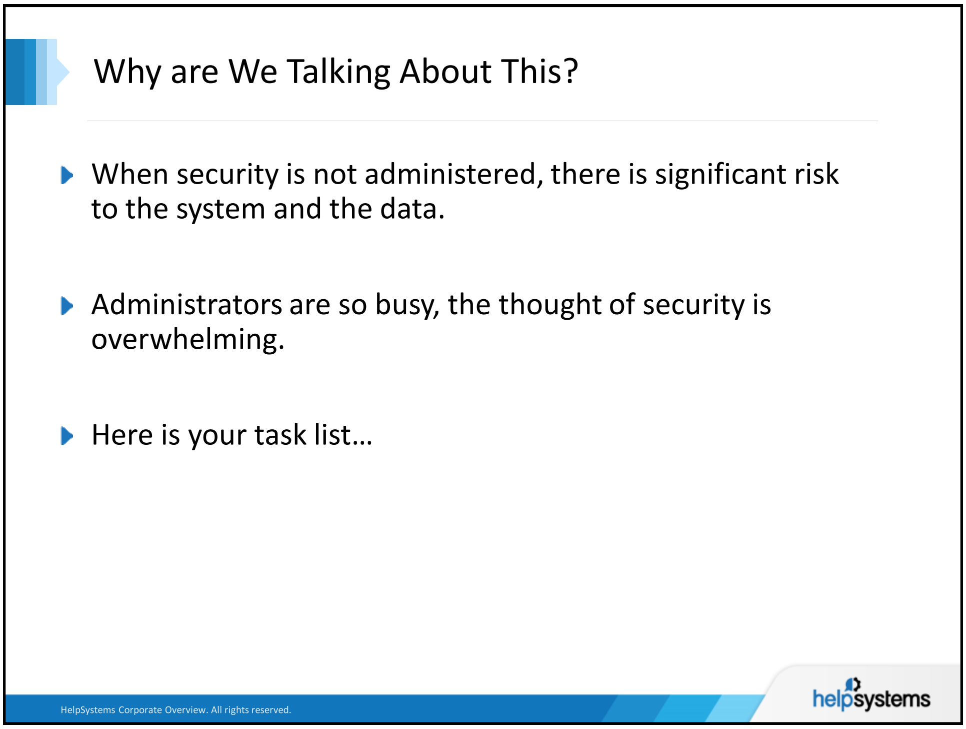
helpsystems

Best Practices for IBM i Security Administration

Carol Woodbury, CISSP, CRISC, PCIP
VP, Global Security Services
Carol.Woodbury@helpsystems.com

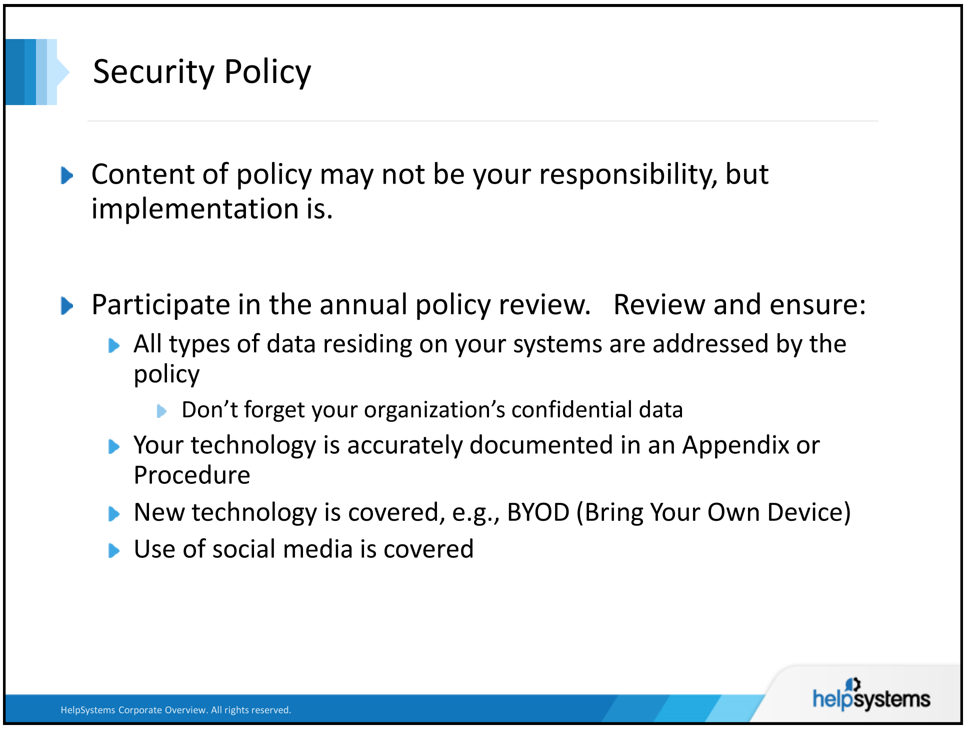
www.helpsystems.com



Why are We Talking About This?

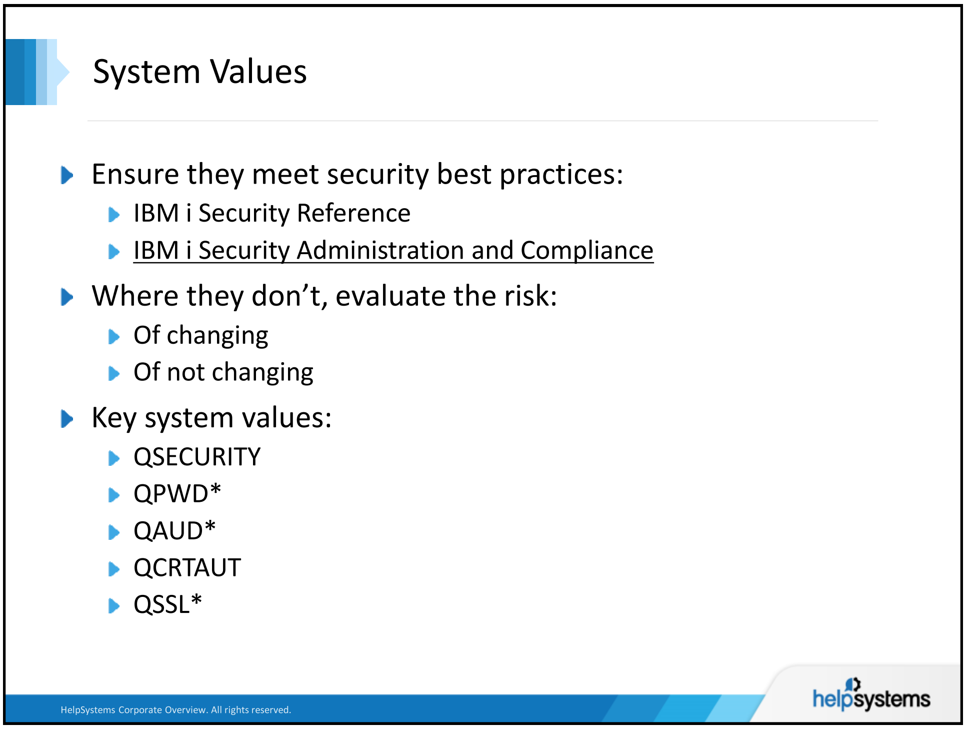
- When security is not administered, there is significant risk to the system and the data.
- Administrators are so busy, the thought of security is overwhelming.
- Here is your task list…

helpsystems



Security Policy

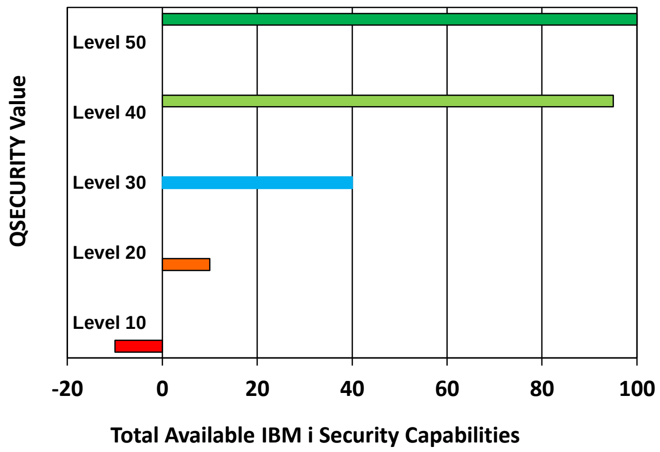
- Content of policy may not be your responsibility, but implementation is.
- Participate in the annual policy review.   Review and ensure:
  - All types of data residing on your systems are addressed by the policy
    - Don’t forget your organization’s confidential data
  - Your technology is accurately documented in an Appendix or Procedure
  - New technology is covered, e.g., BYOD (Bring Your Own Device)
  - Use of social media is covered



System Values

- Ensure they meet security best practices:
  - IBM i Security Reference
  - IBM i Security Administration and Compliance
- Where they don’t, evaluate the risk:
  - Of changing
  - Of not changing
- Key system values:
  - QSECURITY
  - QPWD*
  - QAUD*
  - QCRTAUT
  - QSSL*

Security Level (QSECURITY)



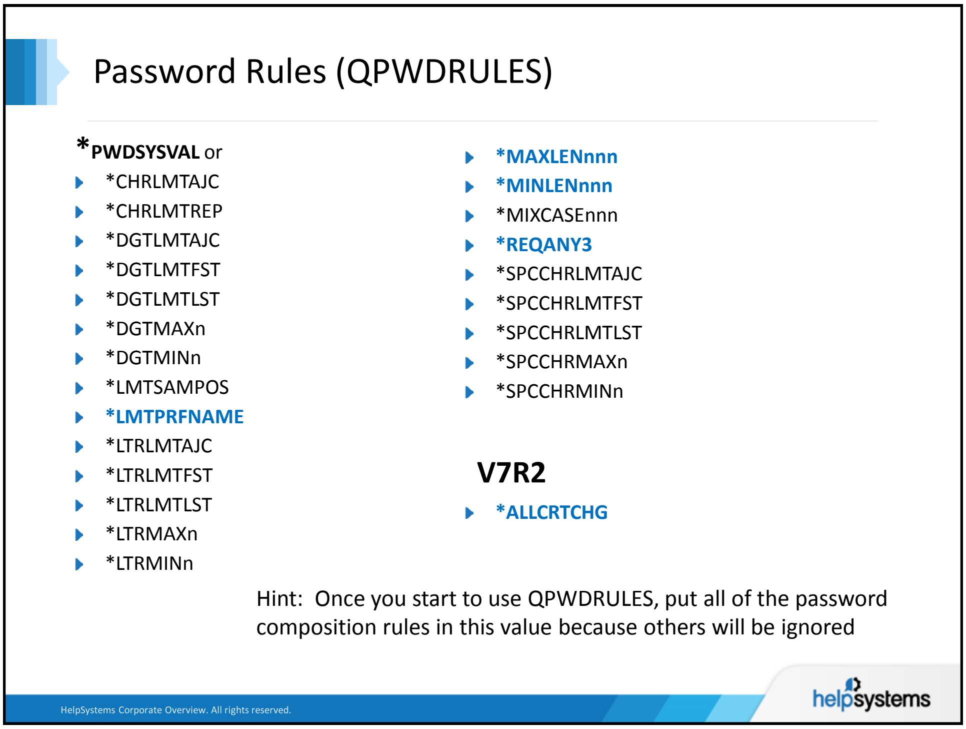
Auditing

QAUDCTL: *AUDLVL, *OBJAUD, *NOQTEMP

QAUDLVL:

- *AUTFAIL
- *CREATE
- *DELETE
- *SAVRST
- *SECCFG
- *SECRUN
- *SERVICE
- *PTFOPR <- V7R2

- For users with command line access, add *CMD auditing
  - CHGUSRAUD
- To monitor when a profile is used, add *JOBBAS
  - CHGUSRAUD
- Manage journal receivers:
  - Have a complete set of receivers
  - So specific date(s) can easily be retrieved
  - Know your compliance requirements! ⬅



Password Rules (QPWDRULES)

***PWDSYSVAL** or

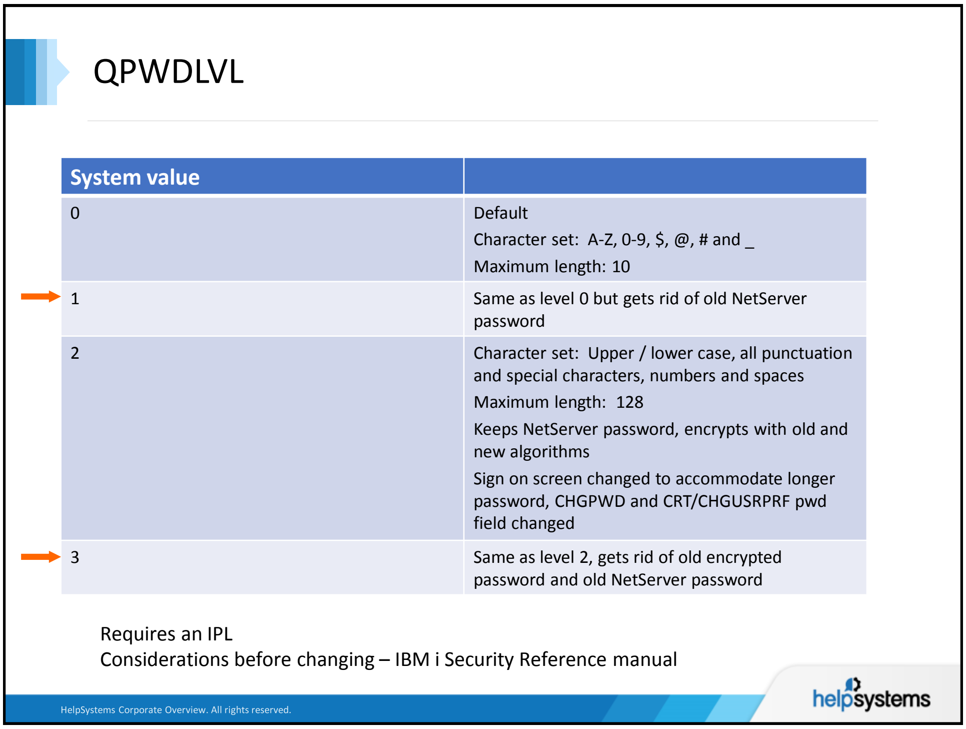
- *CHRLMTAJC
- *CHRLMTREP
- *DGTLMTAJC
- *DGTLMTFST
- *DGTLMTLST
- *DGTMAXn
- *DGTMINn
- *LMTSAMPOS
- ***LMTPRFNAME**
- *LTRLMTAJC
- *LTRLMTFST
- *LTRLMTLST
- *LTRMAXn
- *LTRMINn

- ***MAXLENnnn**
- ***MINLENnnn**
- *MIXCASEnnn
- ***REQANY3**
- *SPCCHRLMTAJC
- *SPCCHRLMTFST
- *SPCCHRLMTLST
- *SPCCHRMAXn
- *SPCCHRMINn

V7R2

- ***ALLCRTCHG**

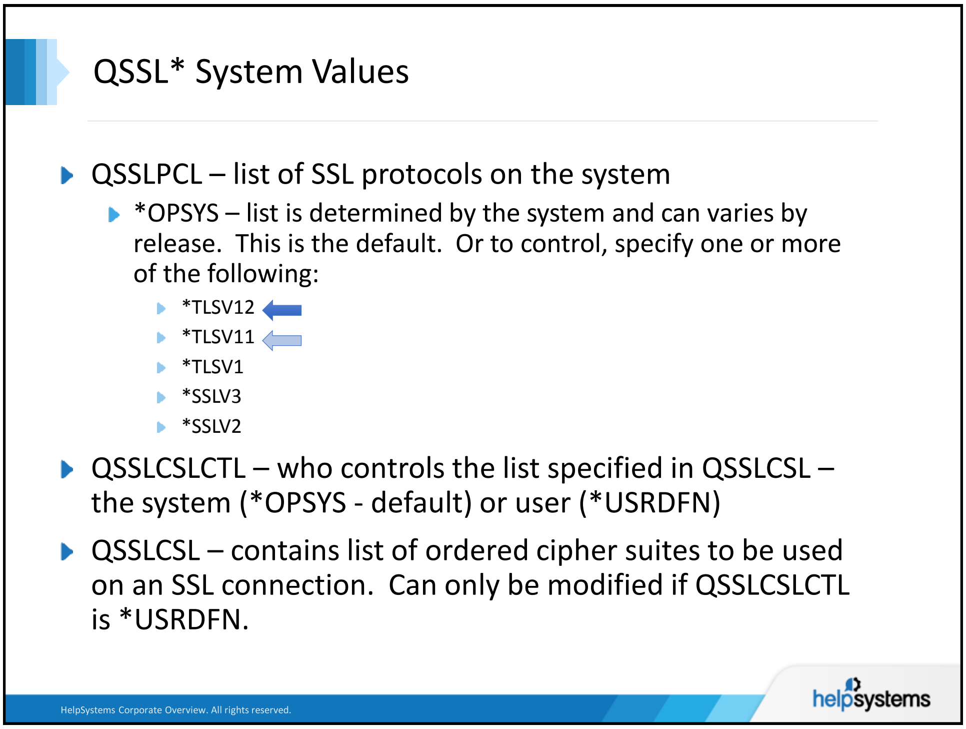
Hint: Once you start to use QPWDRULES, put all of the password composition rules in this value because others will be ignored



QPWDLVL

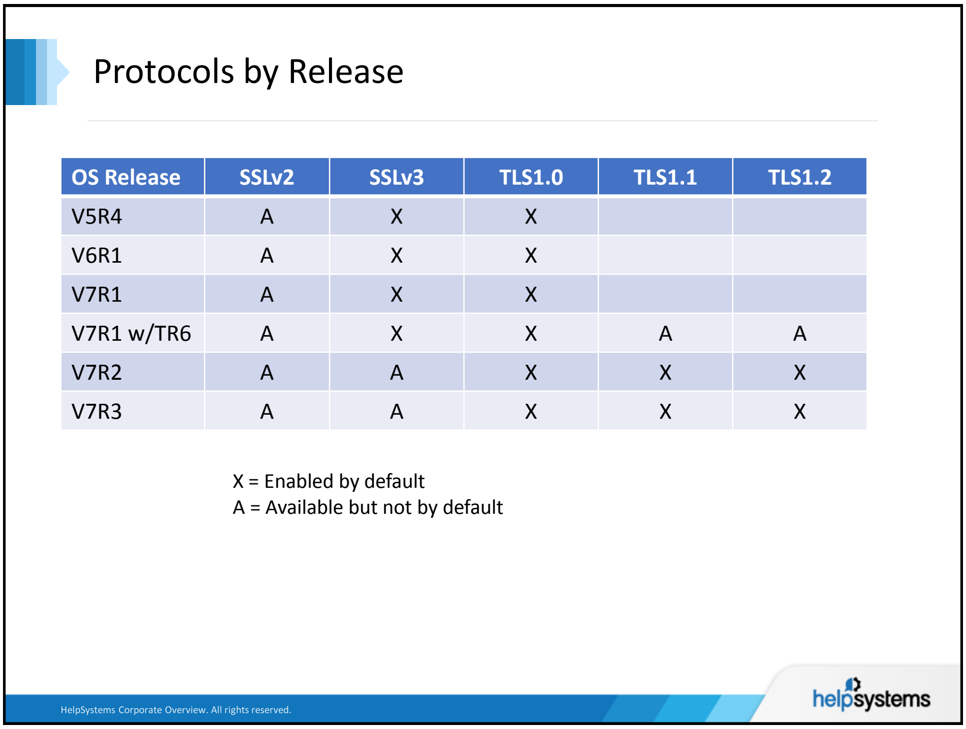
System value	
0	Default Character set: A-Z, 0-9, $, @, # and _ Maximum length: 10
→ 1	Same as level 0 but gets rid of old NetServer password
2	Character set: Upper / lower case, all punctuation and special characters, numbers and spaces Maximum length: 128 Keeps NetServer password, encrypts with old and new algorithms Sign on screen changed to accommodate longer password, CHGPWD and CRT/CHGUSRPRF pwd field changed
→ 3	Same as level 2, gets rid of old encrypted password and old NetServer password

Requires an IPL
Considerations before changing – IBM i Security Reference manual



QSSL* System Values

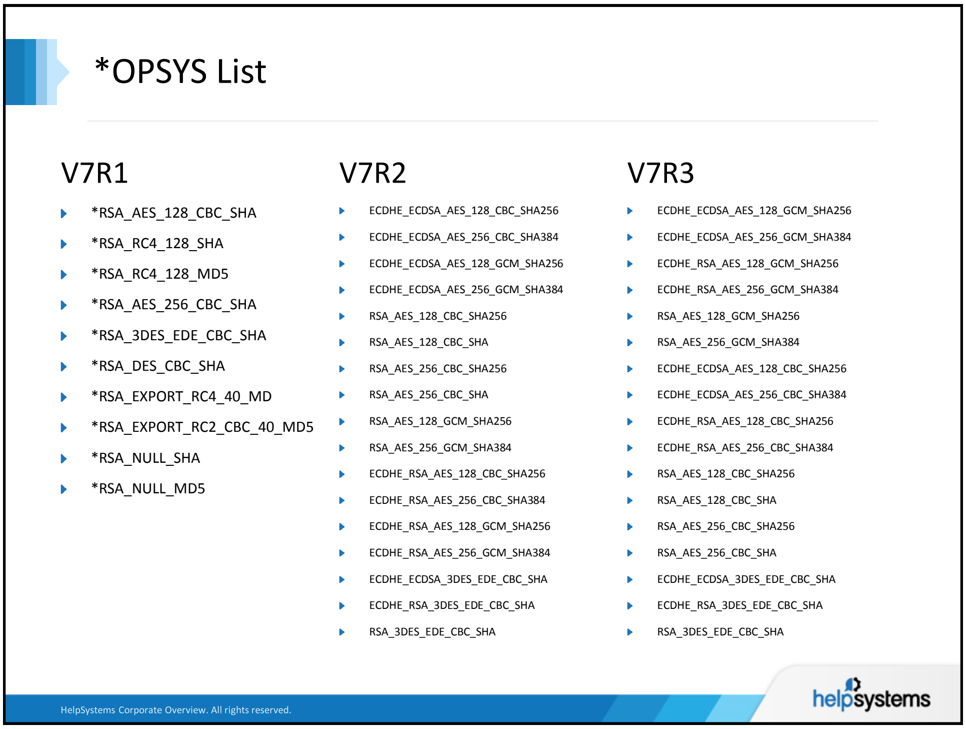
- QSSLPCL – list of SSL protocols on the system
  - *OPSYS – list is determined by the system and can varies by release. This is the default. Or to control, specify one or more of the following:
    - *TLSV12
    - *TLSV11
    - *TLSV1
    - *SSLV3
    - *SSLV2
- QSSLCSLCTL – who controls the list specified in QSSLCSL – the system (*OPSYS - default) or user (*USRDFN)
- QSSLCSL – contains list of ordered cipher suites to be used on an SSL connection. Can only be modified if QSSLCSLCTL is *USRDFN.



Protocols by Release

OS Release	SSLv2	SSLv3	TLS1.0	TLS1.1	TLS1.2
V5R4	A	X	X		
V6R1	A	X	X		
V7R1	A	X	X		
V7R1 w/TR6	A	X	X	A	A
V7R2	A	A	X	X	X
V7R3	A	A	X	X	X

X = Enabled by default
A = Available but not by default



*OPSYS List

V7R1

- *RSA_AES_128_CBC_SHA
- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_AES_256_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC4_40_MD
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_NULL_SHA
- *RSA_NULL_MD5

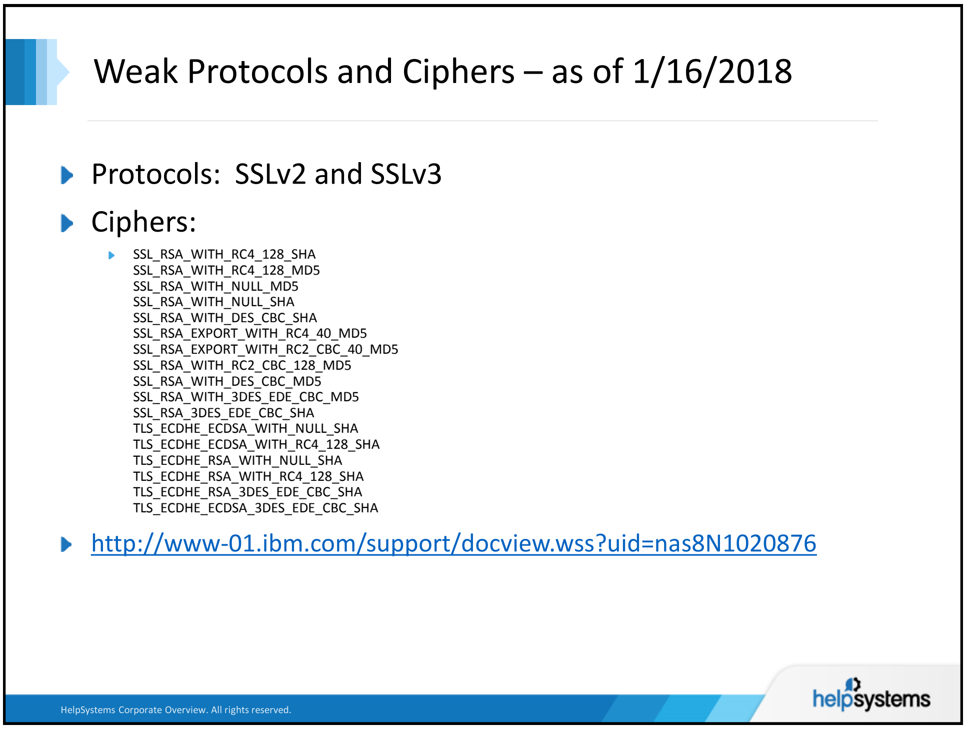
V7R2

- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- RSA_AES_128_CBC_SHA256
- RSA_AES_128_CBC_SHA
- RSA_AES_256_CBC_SHA256
- RSA_AES_256_CBC_SHA
- RSA_AES_128_GCM_SHA256
- RSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384
- ECDHE_ECDSA_3DES_EDE_CBC_SHA
- ECDHE_RSA_3DES_EDE_CBC_SHA
- RSA_3DES_EDE_CBC_SHA

V7R3

- ECDHE_ECDSA_AES_128_GCM_SHA256
- ECDHE_ECDSA_AES_256_GCM_SHA384
- ECDHE_RSA_AES_128_GCM_SHA256
- ECDHE_RSA_AES_256_GCM_SHA384
- RSA_AES_128_GCM_SHA256
- RSA_AES_256_GCM_SHA384
- ECDHE_ECDSA_AES_128_CBC_SHA256
- ECDHE_ECDSA_AES_256_CBC_SHA384
- ECDHE_RSA_AES_128_CBC_SHA256
- ECDHE_RSA_AES_256_CBC_SHA384
- RSA_AES_128_CBC_SHA256
- RSA_AES_128_CBC_SHA
- RSA_AES_256_CBC_SHA256
- RSA_AES_256_CBC_SHA
- ECDHE_ECDSA_3DES_EDE_CBC_SHA
- ECDHE_RSA_3DES_EDE_CBC_SHA
- RSA_3DES_EDE_CBC_SHA

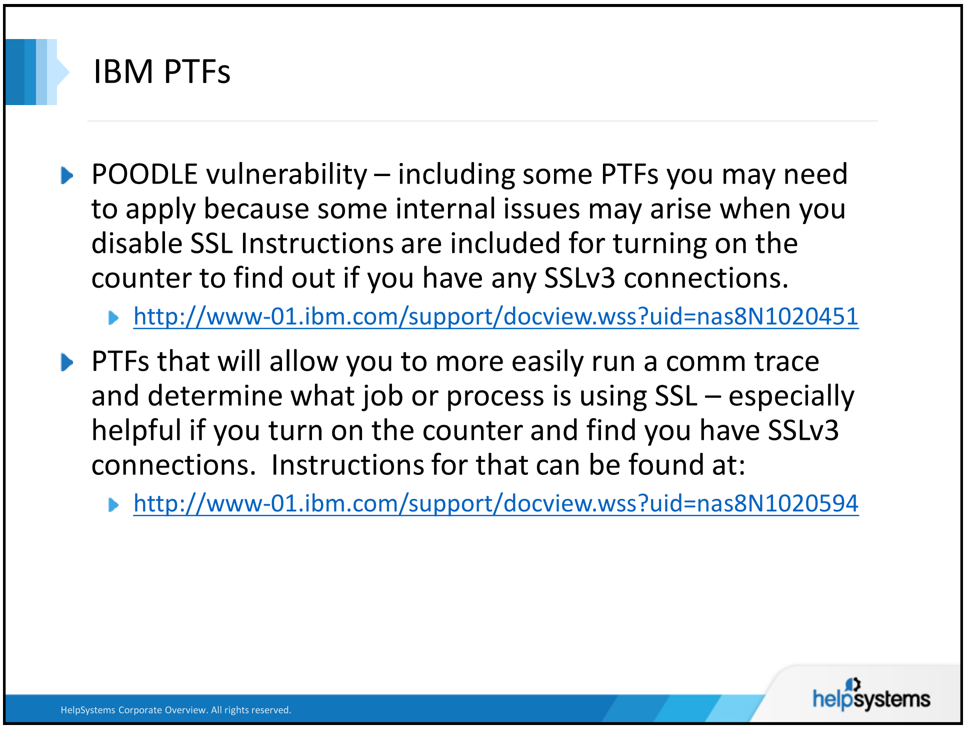
HelpSystems Corporate Overview. All rights reserved.



Weak Protocols and Ciphers – as of 1/16/2018

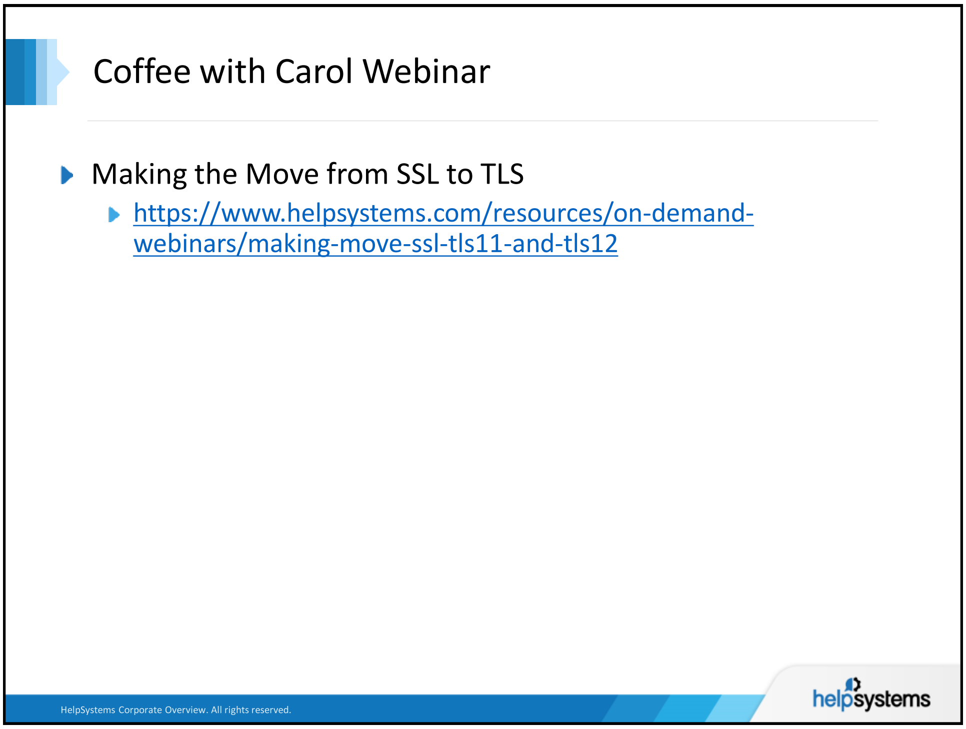
- Protocols: SSLv2 and SSLv3
- Ciphers:
  - SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_RC4_128_MD5
    SSL_RSA_WITH_NULL_MD5
    SSL_RSA_WITH_NULL_SHA
    SSL_RSA_WITH_DES_CBC_SHA
    SSL_RSA_EXPORT_WITH_RC4_40_MD5
    SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
    SSL_RSA_WITH_RC2_CBC_128_MD5
    SSL_RSA_WITH_DES_CBC_MD5
    SSL_RSA_WITH_3DES_EDE_CBC_MD5
    SSL_RSA_3DES_EDE_CBC_SHA
    TLS_ECDHE_ECDSA_WITH_NULL_SHA
    TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
    TLS_ECDHE_RSA_WITH_NULL_SHA
    TLS_ECDHE_RSA_WITH_RC4_128_SHA
    TLS_ECDHE_RSA_3DES_EDE_CBC_SHA
    TLS_ECDHE_ECDSA_3DES_EDE_CBC_SHA
- http://www-01.ibm.com/support/docview.wss?uid=nas8N1020876

HelpSystems Corporate Overview. All rights reserved.



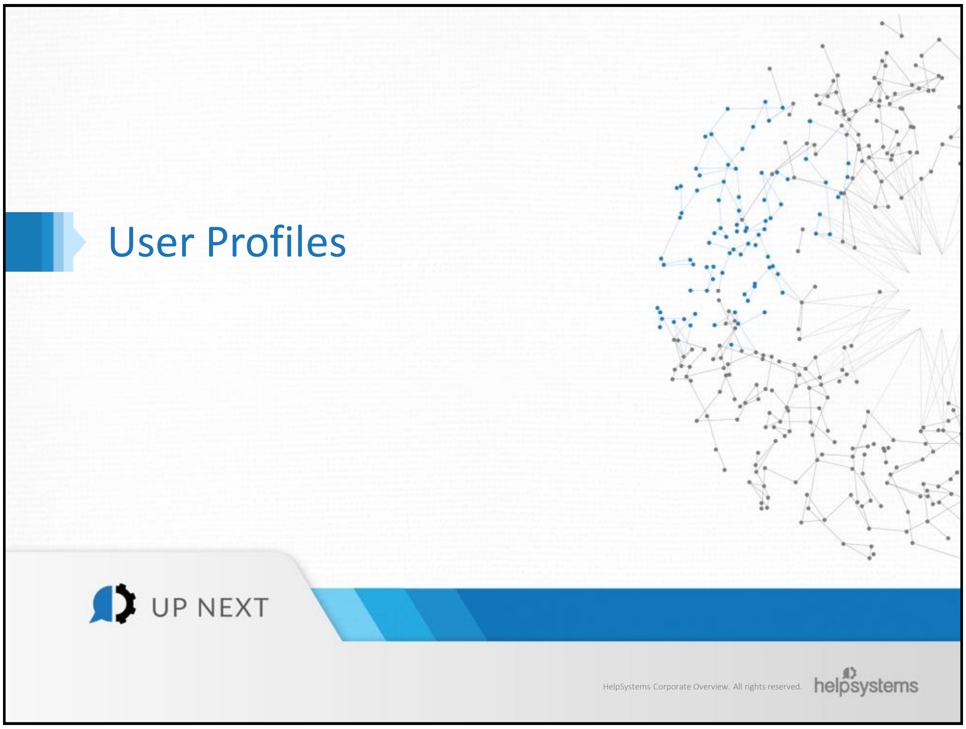
IBM PTFs

- POODLE vulnerability – including some PTFs you may need to apply because some internal issues may arise when you disable SSL Instructions are included for turning on the counter to find out if you have any SSLv3 connections.
  - http://www-01.ibm.com/support/docview.wss?uid=nas8N1020451
- PTFs that will allow you to more easily run a comm trace and determine what job or process is using SSL – especially helpful if you turn on the counter and find you have SSLv3 connections. Instructions for that can be found at:
  - http://www-01.ibm.com/support/docview.wss?uid=nas8N1020594



Coffee with Carol Webinar

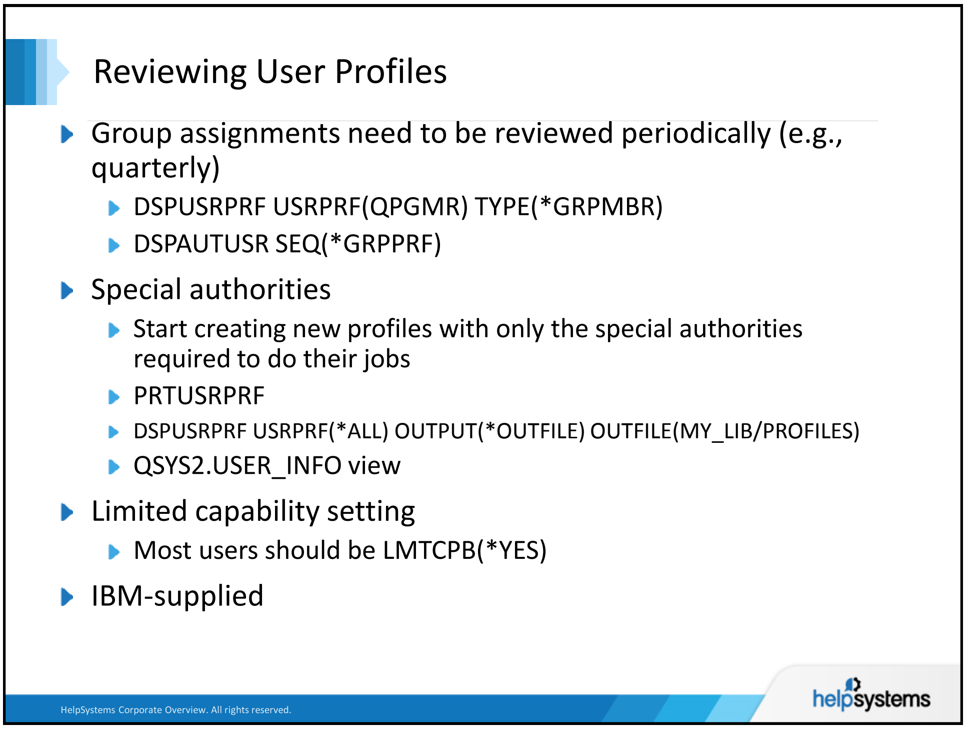
- Making the Move from SSL to TLS
  - https://www.helpsystems.com/resources/on-demand-webinars/making-move-ssl-tls11-and-tls12



User Profiles

UP NEXT

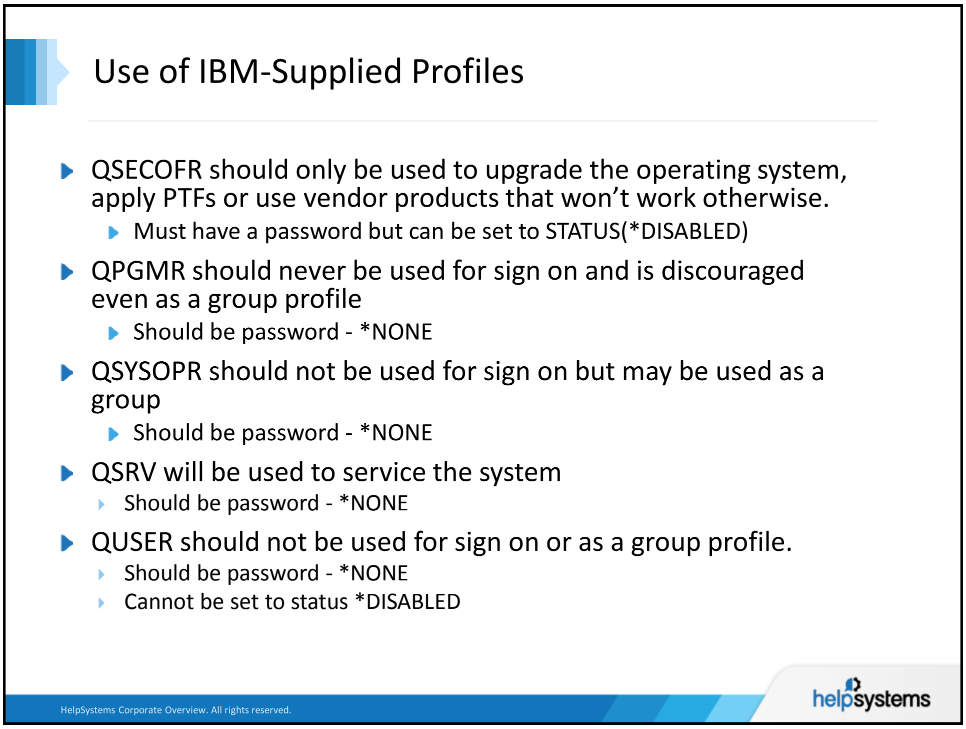
HelpSystems Corporate Overview. All rights reserved.



Reviewing User Profiles

- Group assignments need to be reviewed periodically (e.g., quarterly)
  - DSPUSRPRF USRPRF(QPGMR) TYPE(*GRPMBR)
  - DSPAUTUSR SEQ(*GRPPRF)
- Special authorities
  - Start creating new profiles with only the special authorities required to do their jobs
  - PRTUSRPRF
  - DSPUSRPRF USRPRF(*ALL) OUTPUT(*OUTFILE) OUTFILE(MY_LIB/PROFILES)
  - QSYS2.USER_INFO view
- Limited capability setting
  - Most users should be LMTCPB(*YES)
- IBM-supplied

HelpSystems Corporate Overview. All rights reserved.

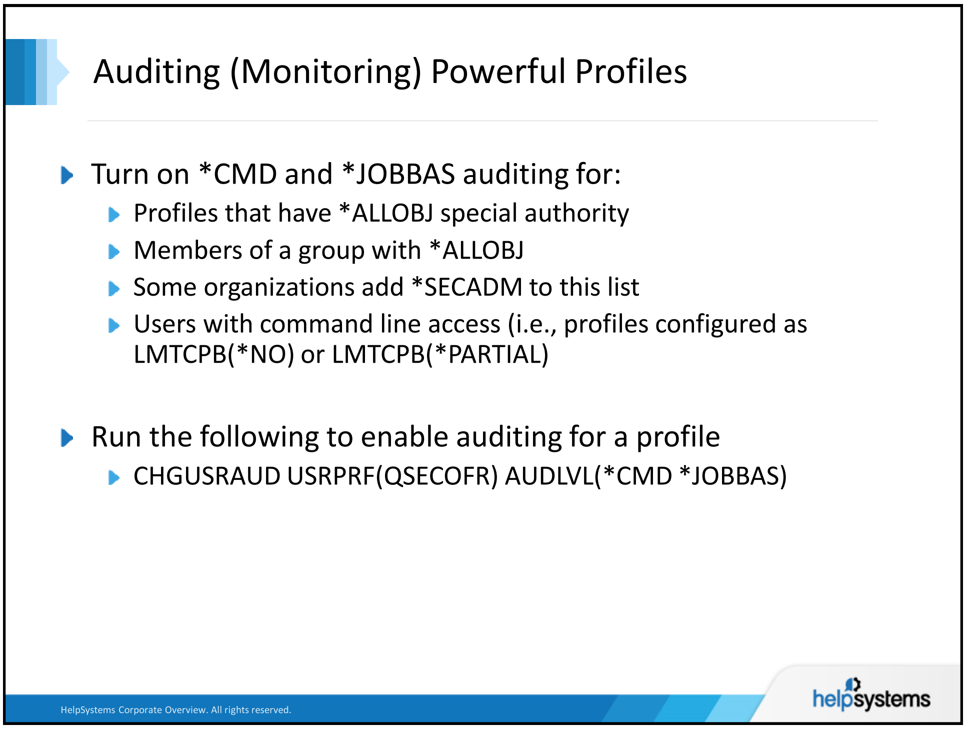


Use of IBM-Supplied Profiles

- QSECOFR should only be used to upgrade the operating system, apply PTFs or use vendor products that won’t work otherwise.
  - Must have a password but can be set to STATUS(*DISABLED)
- QPGMR should never be used for sign on and is discouraged even as a group profile
  - Should be password - *NONE
- QSYSOPR should not be used for sign on but may be used as a group
  - Should be password - *NONE
- QSRV will be used to service the system
  - Should be password - *NONE
- QUSER should not be used for sign on or as a group profile.
  - Should be password - *NONE
  - Cannot be set to status *DISABLED

HelpSystems Corporate Overview. All rights reserved.

helpsystems

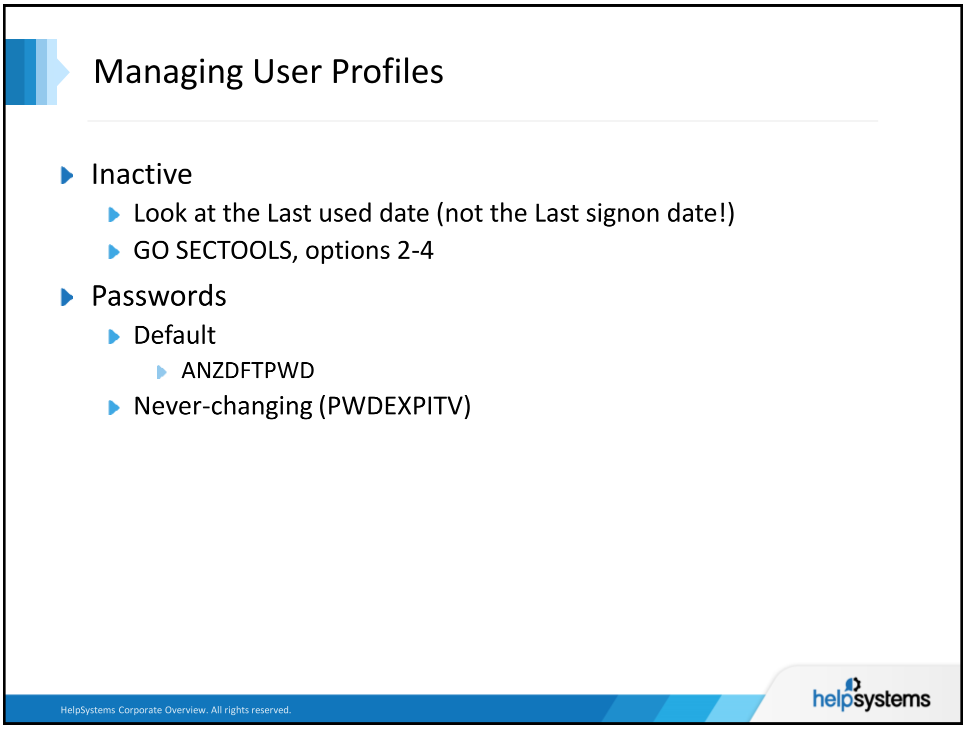


Auditing (Monitoring) Powerful Profiles

- Turn on *CMD and *JOBBAS auditing for:
  - Profiles that have *ALLOBJ special authority
  - Members of a group with *ALLOBJ
  - Some organizations add *SECADM to this list
  - Users with command line access (i.e., profiles configured as LMTCPB(*NO) or LMTCPB(*PARTIAL)
- Run the following to enable auditing for a profile
  - CHGUSRAUD USRPRF(QSECOFR) AUDLVL(*CMD *JOBBAS)

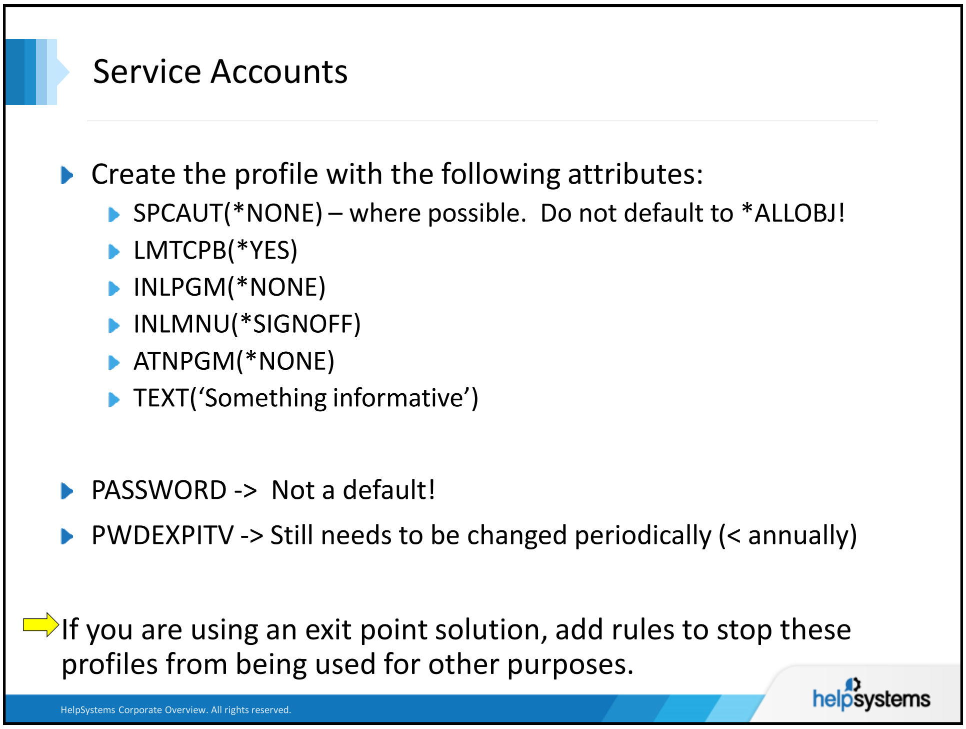
HelpSystems Corporate Overview. All rights reserved.

helpsystems



Managing User Profiles

- Inactive
  - Look at the Last used date (not the Last signon date!)
  - GO SECTOOLS, options 2-4
- Passwords
  - Default
    - ANZDFTPWD
  - Never-changing (PWDEXPITV)

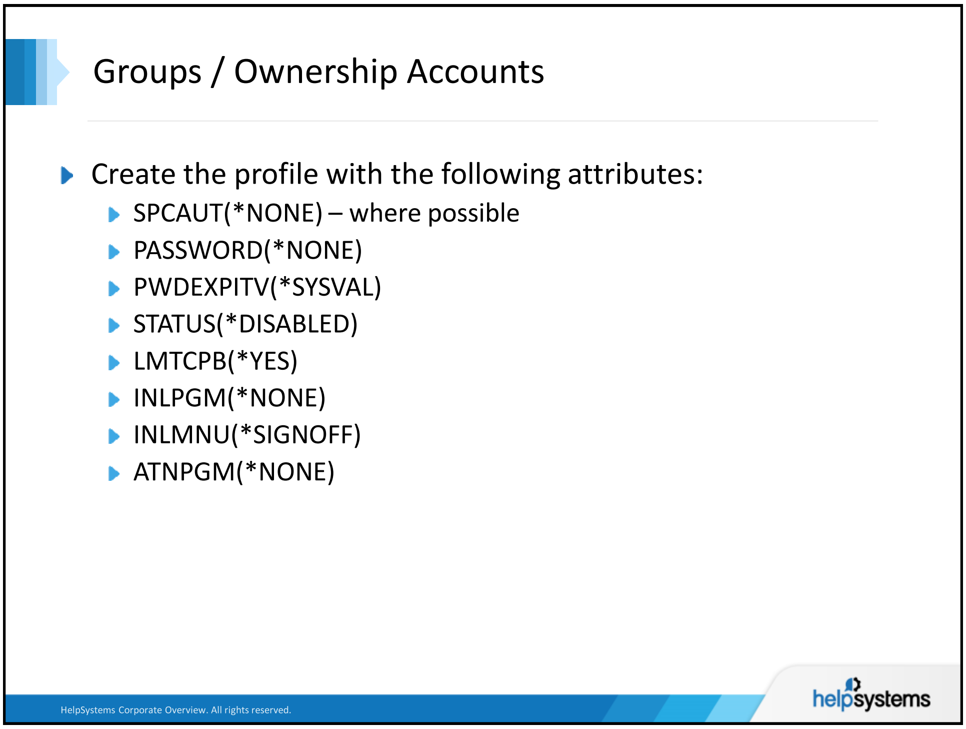


Service Accounts

- Create the profile with the following attributes:
  - SPCAUT(*NONE) – where possible. Do not default to *ALLOBJ!
  - LMTCPB(*YES)
  - INLPGM(*NONE)
  - INLMNU(*SIGNOFF)
  - ATNPGM(*NONE)
  - TEXT(‘Something informative’)

- PASSWORD -> Not a default!
- PWDEXPITV -> Still needs to be changed periodically (< annually)

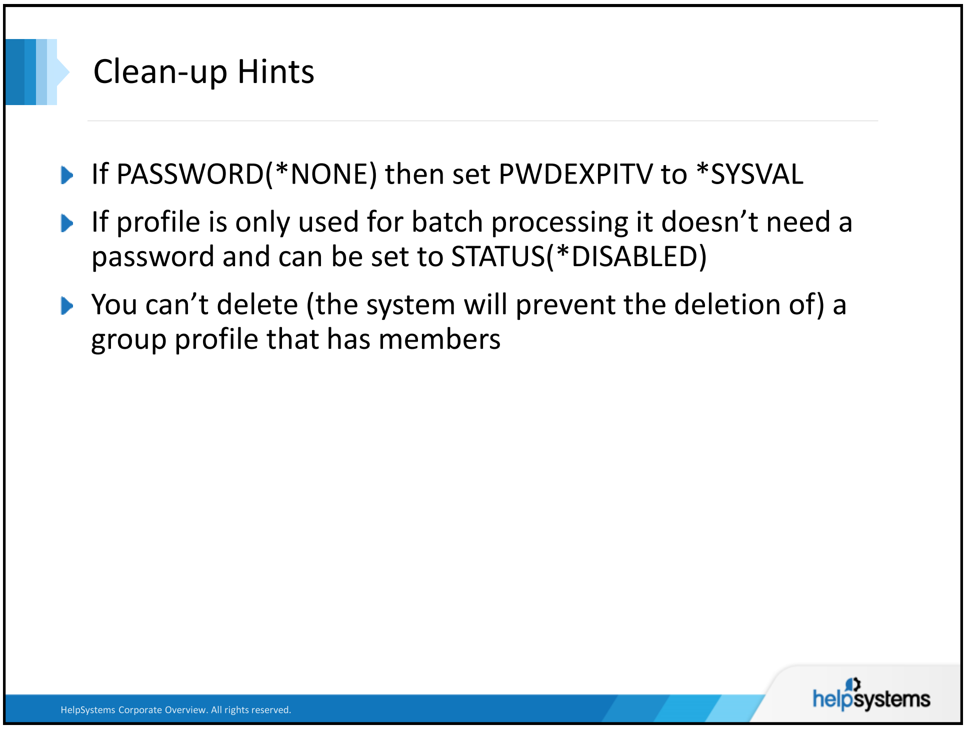
⇨If you are using an exit point solution, add rules to stop these profiles from being used for other purposes.



Groups / Ownership Accounts

- Create the profile with the following attributes:
  - SPCAUT(*NONE) – where possible
  - PASSWORD(*NONE)
  - PWDEXPITV(*SYSVAL)
  - STATUS(*DISABLED)
  - LMTCPB(*YES)
  - INLPGM(*NONE)
  - INLMNU(*SIGNOFF)
  - ATNPGM(*NONE)

HelpSystems Corporate Overview. All rights reserved.



Clean-up Hints

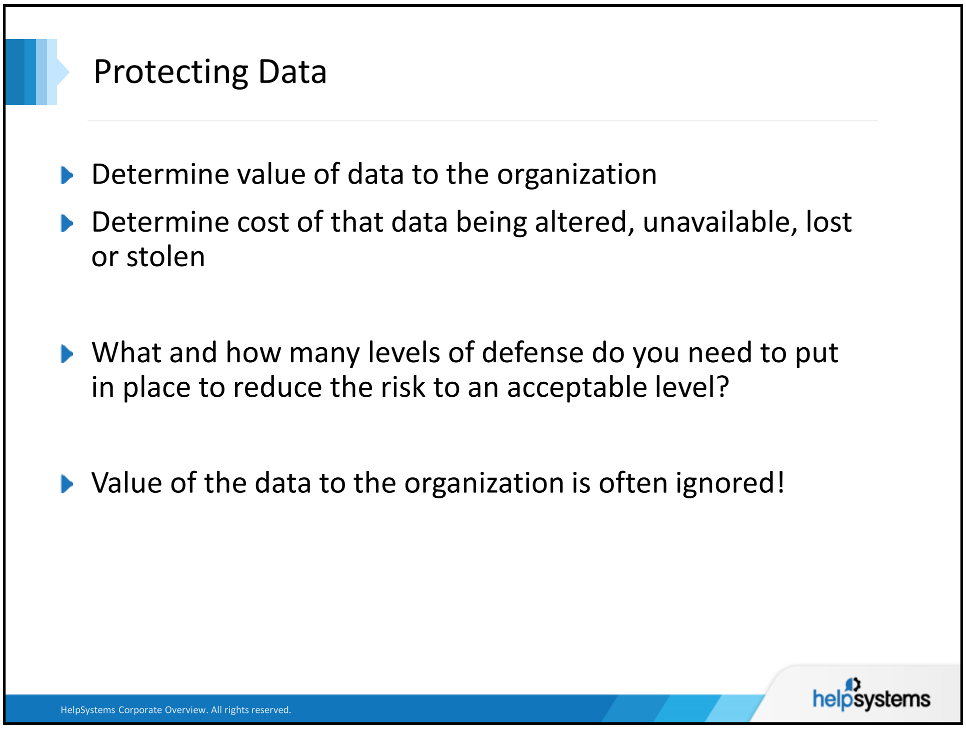
- If PASSWORD(*NONE) then set PWDEXPITV to *SYSVAL
- If profile is only used for batch processing it doesn't need a password and can be set to STATUS(*DISABLED)
- You can't delete (the system will prevent the deletion of) a group profile that has members

HelpSystems Corporate Overview. All rights reserved.

Protecting Data

UP NEXT

HelpSystems Corporate Overview. All rights reserved.



Protecting Data

- Determine value of data to the organization
- Determine cost of that data being altered, unavailable, lost or stolen
- What and how many levels of defense do you need to put in place to reduce the risk to an acceptable level?
- Value of the data to the organization is often ignored!

HelpSystems Corporate Overview. All rights reserved.

Security Must be More than Menu ‘Security’

J.D. Edwards & Company

Selection or command

Users downloading to an Excel spreadsheet

JDBC connections to WebSphere applications

FTP to banks, payroll processors, trading partners

Developers updating data

Users running SQL or Queries

DDM

Administrators and Analysts with legitimate command line access

Secure the Data

- Start by considering how the data should be secured
  - For Integrity -> *PUBLIC(*USE)
  - For Confidentiality -> *PUBLIC(*EXCLUDE)
- Determine how to secure the data without breaking other applications
- Implement object level security

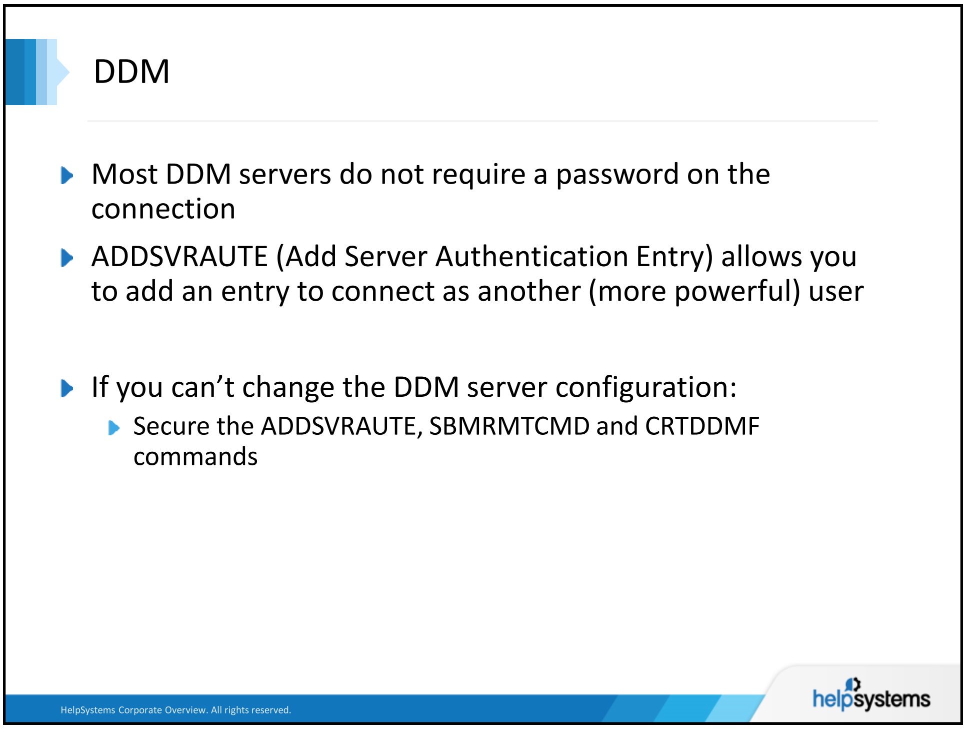
Authorization Lists

- Review (at least quarterly), profiles authorized to authorization lists
  - DSPAUTL
  - QSYS2.AUTHORIZATION_LIST_USER_INFO
- May also want to review objects secured by the list
  - DSPAUTLOBJ
  - QSYS2.AUTHORIZATION_LIST_INFO
  - https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM%20i%20Technology%20Updates/page/DB2%20for%20i%20-%20Services

Adopted Authority

- Not dangerous as long as it's used wisely
- Need process in place to review programs that adopt – especially an *ALLOBJ profile

- Be wary of:
  - Programs that put up a command line (set Use adopted authority to *NO and User profile to *USER)
  - Menu options that call an IBM command – WRKSPLF, WRKQRY, STRSQL (may been to add them to a CL program and set that program to be USEADPAUT(*NO) USRPRF(*USER))
    - PRTADPOBJ



DDM

- Most DDM servers do not require a password on the connection
- ADDSVRAUTE (Add Server Authentication Entry) allows you to add an entry to connect as another (more powerful) user
- If you can't change the DDM server configuration:
  - Secure the ADDSVRAUTE, SBMRMTCMD and CRTDDMF commands

HelpSystems Corporate Overview. All rights reserved.

helpsystems

IFS

UP NEXT

HelpSystems Corporate Overview. All rights reserved.

helpsystems

IFS

- Don’t be afraid of securing the IFS!
- Typically need to:
  - Identify profiles needing to read or write to the directory.
  - Set appropriate *PUBLIC authority
  - Authorized individuals or groups to the directory
- Even without touching objects in the directory … risk is reduced significantly

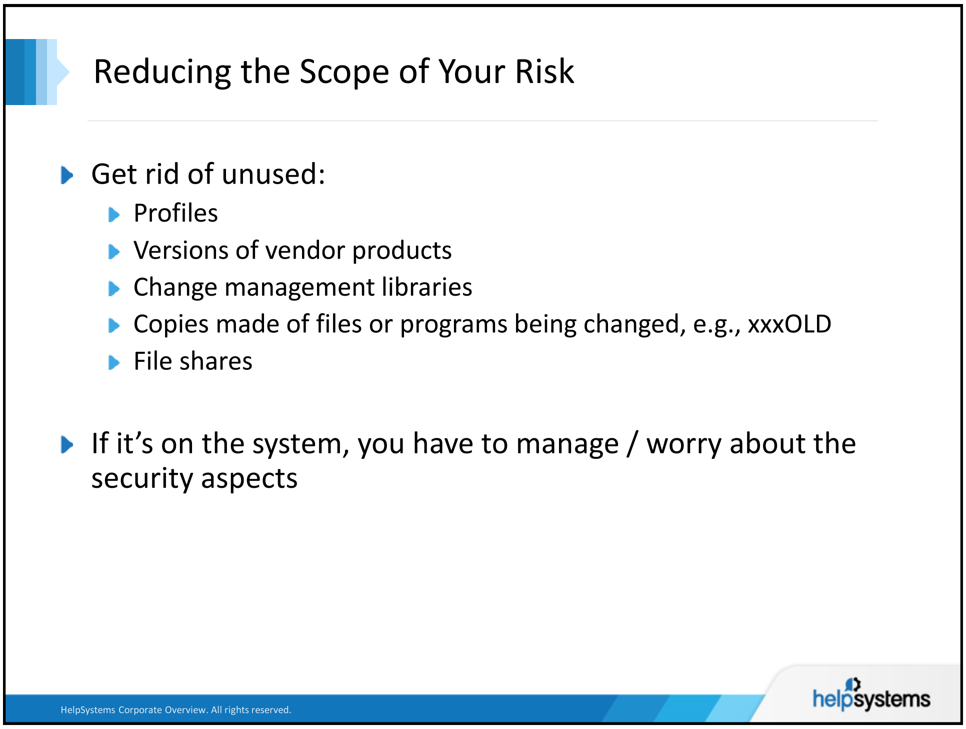
IFS – continued

- Do NOT share root or QSYS.LIB
  - If you MUST share root:
    - Create the share as ‘Read-only’ if possible
    - Create the share name as Name$
    - Use something more obscure than ‘root’ for the name!
    - Use the QPWFSERVER authorization list to protect QSYS.LIB
- Set authority to root:
  - *PUBLIC DTAAUT(*RX) OBJAUT(*NONE)
  - It CANNOT be set to *EXCLUDE!
- Remove guest profiles from the NetServer

Miscellaneous

UP NEXT

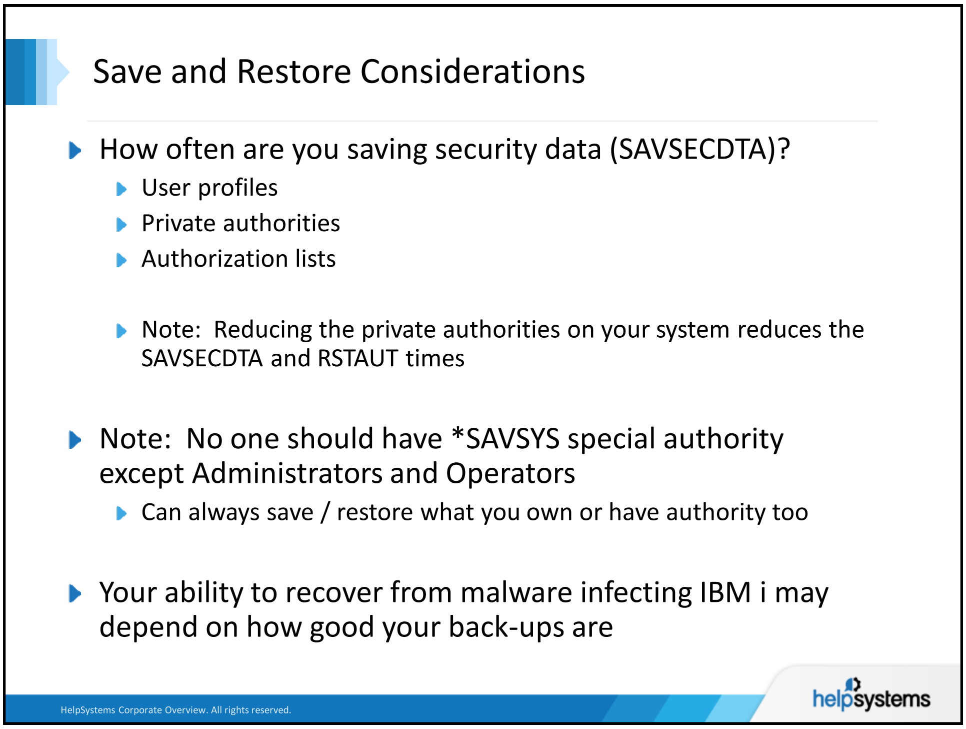
HelpSystems Corporate Overview. All rights reserved. helpsystems



Reducing the Scope of Your Risk

- Get rid of unused:
  - Profiles
  - Versions of vendor products
  - Change management libraries
  - Copies made of files or programs being changed, e.g., xxxOLD
  - File shares
- If it's on the system, you have to manage / worry about the security aspects

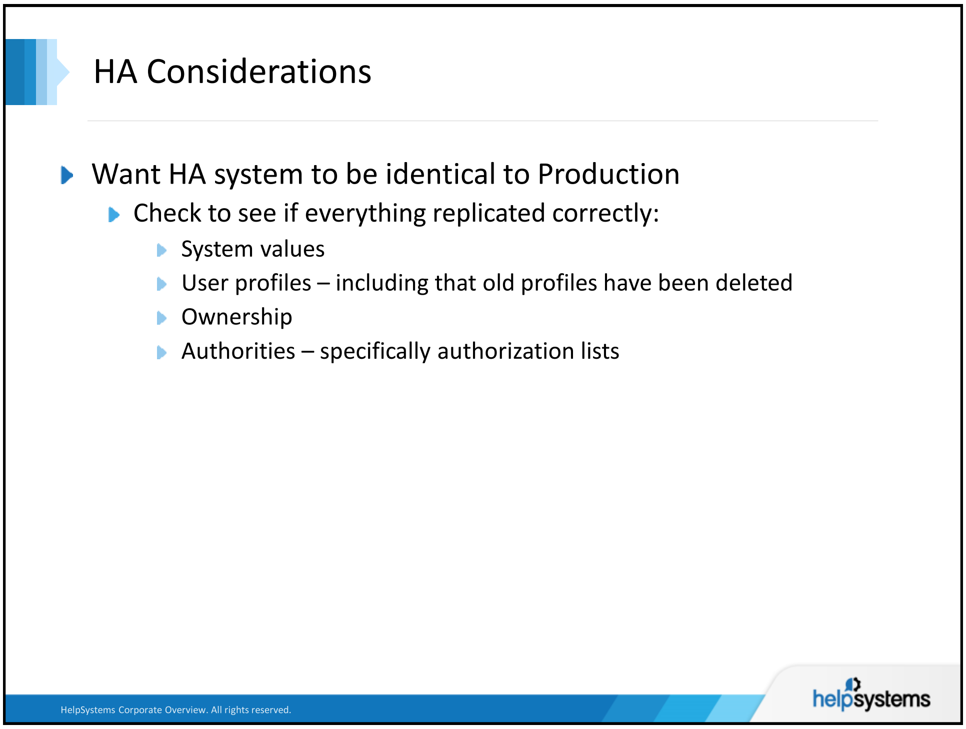
HelpSystems Corporate Overview. All rights reserved. helpsystems



Save and Restore Considerations

- How often are you saving security data (SAVSECDTA)?
  - User profiles
  - Private authorities
  - Authorization lists
  - Note: Reducing the private authorities on your system reduces the SAVSECDTA and RSTAUT times
- Note: No one should have *SAVSYS special authority except Administrators and Operators
  - Can always save / restore what you own or have authority too
- Your ability to recover from malware infecting IBM i may depend on how good your back-ups are

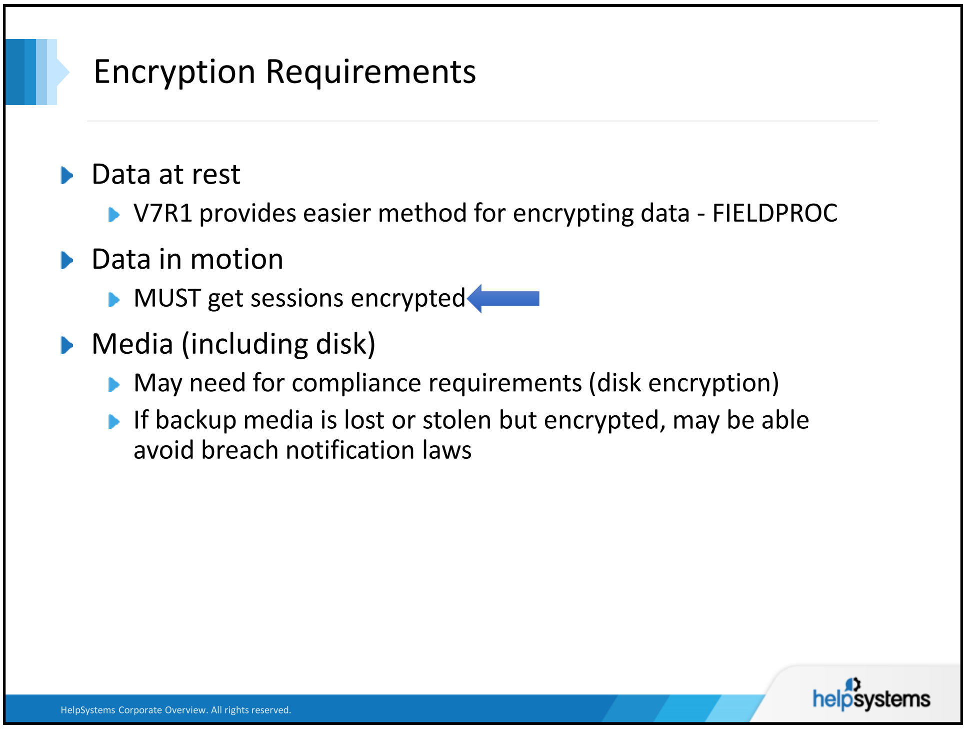
HelpSystems Corporate Overview. All rights reserved.



HA Considerations

- Want HA system to be identical to Production
  - Check to see if everything replicated correctly:
    - System values
    - User profiles – including that old profiles have been deleted
    - Ownership
    - Authorities – specifically authorization lists

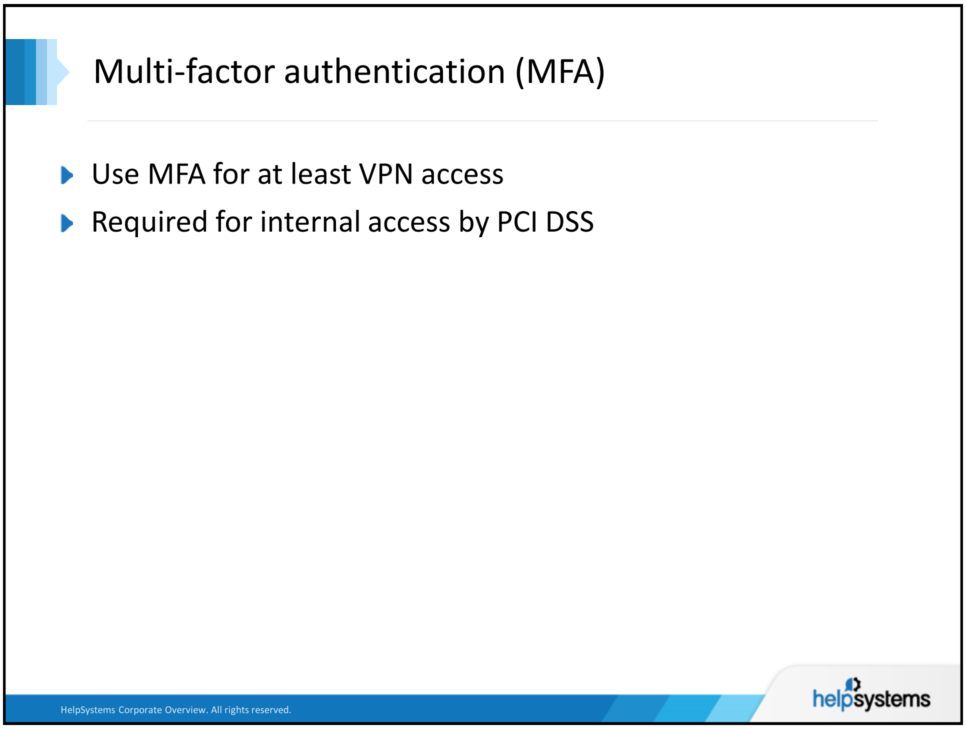
HelpSystems Corporate Overview. All rights reserved.



Encryption Requirements

- Data at rest
  - V7R1 provides easier method for encrypting data - FIELDPROC
- Data in motion
  - MUST get sessions encrypted
- Media (including disk)
  - May need for compliance requirements (disk encryption)
  - If backup media is lost or stolen but encrypted, may be able avoid breach notification laws

HelpSystems Corporate Overview. All rights reserved.



Multi-factor authentication (MFA)

- Use MFA for at least VPN access
- Required for internal access by PCI DSS

HelpSystems Corporate Overview. All rights reserved.

Stay Current!

- OS level
  - Many security enhancements – including protocols and cipher suites that may be needed for compliance - aren’t available in lower releases.
  - V7R1 goes out of support –April 2018
- Technology Refresh
  - https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM%20i%20Technology%20Updates/page/IBM%20i%20Technology%20Updates
- PTFs
  - Java
  - Open source
  - Use the SYSTOOLS.GROUP_PTF_CURRENCY
    - https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/IBM%20i%20Technology%20Updates/page/DB2%20for%20i%20-%20Services
- iAccess -> Access Client Solutions

Where do you Start?

- Perform a Risk (Vulnerability) Assessment
  - “Security starts with an Assessment”
- Even if you are reviewing settings on a regular basis, a vulnerability assessment will look at things you’re not considering.
- Like going to a doctor for a physical, the vulnerability assessment should be done by a security expert
  - You will always check the things you know to check
- Provides you with a list of work items

By now, this might be how your brain feels…!

Goal

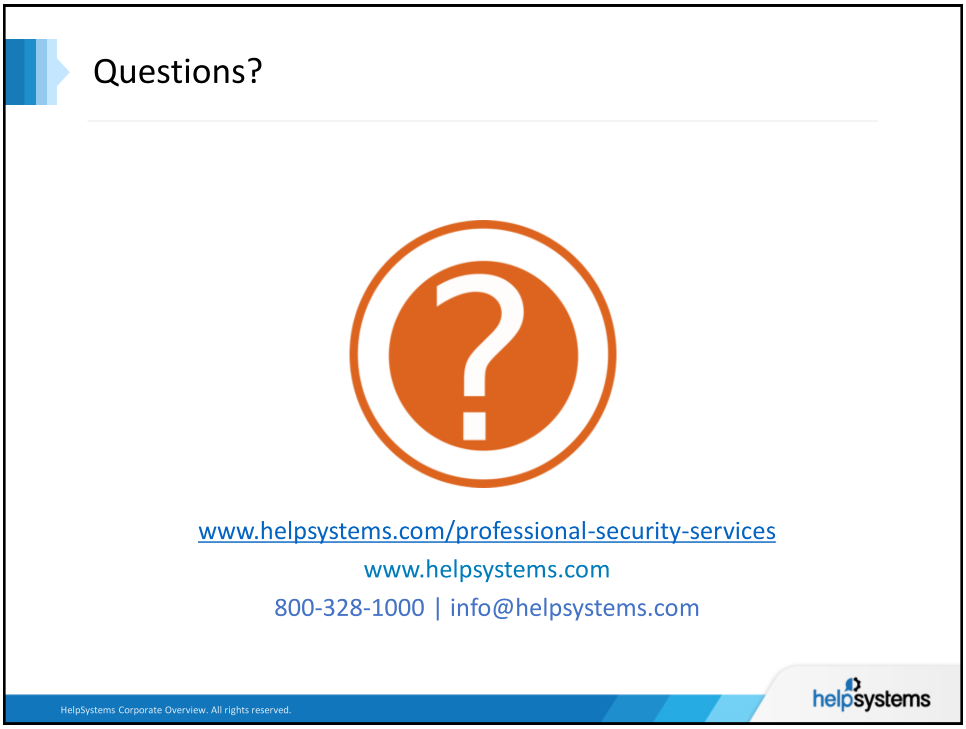
Reduce Risk!

Start Somewhere – Even if It's a Small Step!

For more information

- IBM i Security Reference manual
- https://www.ibm.com/support/knowledgecenter/api/content/nl/en-us/ssw_ibm_i_73/rzarl/sc415302.pdf
  - Chapter 2 – Moving between security levels
  - Chapter 3 – System values
  - Chapter 6 – Securing printed output
  - Chapter 9 – Auditing (as well as Appendix E and F)
  - Chapter 10 – Authority Collection (new in V7R3)
  - Appendix B – IBM-supplied profiles
  - Appendix D – Authority needed to run CL commands

- IBM i Security Administration and Compliance, 2nd edition, by Carol Woodbury, MC Press Online, 2016.



Questions?

www.helpsystems.com/professional-security-services

www.helpsystems.com

800-328-1000 | info@helpsystems.com