EASTERN
DATACOMM

Your Trusted Partner for
Customized Safety and Communications Solutions

Video Surveillance Comparison Checklist

To comply with current legislation, schools, businesses, and government entities across the country need to rip and replace non-compliant video surveillance cameras because these devices contain specific chip sets that contain malicious "back doors". These entry points allow the manufacturer or their affiliates to view and collect data from the cameras and other devices that contain these specific chipsets.

What You Should Know about Removing These Cameras and Chips

✓ Yes. These Cameras Need to Be Removed.

You will need to remove any cameras that don't meet the National Defense Authorization Act (NDAA) in order to comply. This is especially true if these projects were funded by the government (inclusive of federal grant money) or if the buildings or grounds that are using this equipment received government funding.

✓ Yes. This Will Enhance Your Safety Profile.

Removing and replacing these banned cameras will enhance your organization's safety and security as it ensures greater privacy for those within the surveilled location.

✓ Yes. The Banned Cameras Present a Real Risk to Confidentiality.

Replacing banned cameras can also prevent the unintended sharing of confidential information, and the risks of non-compliant equipment loom more ominously as a real threat.

✗ No. Not All Video Surveillance Cameras Are Banned.

This particular ban is for a select group of silicon manufacturers that produce the chipsets, all of which are located within China. Consult our Eastern DataComm team to learn if your video surveillance system is affected by the rip-and-replace requirement.

✓ Do: Double-Check Your Manufacturers.

There are a few manufacturers to be wary of, including Hangzhou Hikvision Digital Technology Company and Dahua Technology Company. Many subsidiary or affiliate manufacturers have rebranded models that look different, but contain the same chipsets. So be a discerning consumer or reach out to the Eastern DataComm team for help.

✓ Do: Navigate These Changes with a Credible Technology Partner.

The market is shifting. Manufacturers are responding to the desire for compliant solutions. That said, working with a trusted vendor partner who can discern the difference between compliant and non-compliant solutions remains the best way to avoid unknowingly purchasing and installing non-compliant devices.

✗ Don't: Be Too Quick to Jump on a "Great Deal".

Non-NDAA-compliant cameras are typically less expensive, costing about a quarter the price of the competitors that are NDAA-compliant, which has made them a very affordable choice. But that initial savings comes with a high security risk.

Best Practices for Video Surveillance for Your Organization

✓ **Consult the Experts**: Consult a safety expert and conduct a physical walkthrough of your buildings and grounds. These experts have the knowledge and experience to give you insight into camera placement and answer your questions.

✓ **Document Your Process**: As you move through these evaluation and decision stages, be sure to document your current and future camera locations on copies of your floor plans, blueprints, fire evacuation maps, and the like (VMS software, for example).

✓ **Research Your Options**: Be sure to research and understand the main differences between on-prem, cloud, or hybrid solutions. The choice that is right for your campus depends entirely on your unique needs. If you need support in conducting this research, contact a trusted vendor partner like Eastern DataComm. We'll help you find the option that's right for you.

✓ **Take a Multimodal Approach**: Be sure you are utilizing a multimodal approach to alerts. This means using multiple mediums, like email and SMS, to convey important messages to ensure proper notification is received and understood by your intended recipients.

✓ **Plan Proactively**: Configure video pop-ups for actively alerting cameras on the security teams' viewing monitors for immediate response. This will ensure everyone remains on the same page when it matters most.

✗ Don't Go it Alone.

When you're unsure about how to navigate these processes, working with an experienced safety technology advisor like Eastern DataComm facilitates a smooth transition to a fully compliant video surveillance system.

If you'd like to learn more about how our team can help your school or district gain or maintain your video surveillance compliance, contact us here for a Complimentary NDAA Compliance Consultation.

What to Look for in Your Replacement Cameras and Video Surveillance Solutions

✓ Do: Choose a System That Provides Clear and Smooth Coverage.

This is especially helpful for heavily trafficked areas like lobbies, secure areas that hold records, and known problematic nooks where people commonly sequester themselves to conceal their activities from authority figures.

✓ Do: Opt for a Modern System That Utilizes the Latest Technology Available.

Your new system should be modern in terms of its functionality. So, consider whether you can extract data from the cameras using Artificial Intelligence (AI). AI empowers the user to generate proactive alerts based on the video data. Actions and events such as loitering, crowding, or line crossing can be detected in real-time.

✓ Do: Maintain Remote Access to Your Security System.

Be sure to secure and maintain remote access to your physical security system, regardless of device type or geographical location. As an additional precaution, it's also recommended to allocate system functionalities based on role and monitor each user's activity.

✗ Don't: Assume Your Video Surveillance Solution Will Be One-Size-Fits-All.

This means you may need to make use of specialty cameras with specific features. This will allow you to fit these particular areas with equipment that captures meaningful and relevant information.

✗ Don't: Over Complicate Your Video Surveillance System.

Consider ease of use from your planning stage. Accessing your new system should be frictionless, secure, traceable, and when needed, quickly shareable with law enforcement or those who are responsible for building safety and security.

✗ Don't: Forget about Compliance.

Make sure all security systems going forward are NDAA-compliant. This extends beyond IP cameras. This includes physical cameras, NVR/recording server hardware, access control equipment, and the software that controls these systems.

✗ Don't: Make System Updates with Low-Resolution Cameras.

When you're renewing systems, make sure to use high-resolution cameras (4MP) and above for larger spaces. Utilize new AI video analytics to go beyond motion alerts. Create proactive notifications and responses based on these analytics to prevent issues from starting or reoccurring.