NDA Submits Comments for House Overtime Hearing

On Wednesday, NDA submitted comments to the House Committee on Education and Workforce for a subcommittee hearing on the Department of Labor's (DOL) proposed overtime rule. The hearing featured witnesses from various industry sectors and focused on the impact that DOL's proposed rule would have on businesses and the workplace. The DOL has proposed to increase the minimum salary threshold for overtime eligibility by 55% from $35,568 per year to $55,068 per year. The proposal would also implement automatic increases to the threshold every three years, regardless of economic conditions.

In its comments to lawmakers, NDA expressed opposition to DOL's proposed rule and highlighted the negative consequences that could affect employers and employees should the rule be implemented, including:

- limits on career advancement opportunities for employees;
- burdensome labor and compliance costs;
- decreased workplace flexibility and remote work options;
- elimination of middle management positions; and
- declines in employee morale.

NDA also called on Members of Congress to use their influence to urge the Department of Labor to withdraw their proposed rule prior to its implementation. NDA continues to closely monitor DOL's actions on overtime pay and will keep members updated on the latest developments.

IRS Urges Business to Remain Vigilant Against Cyberattacks

As part of National Tax Security Awareness Week, the Internal Revenue Service (IRS) urged businesses to remain vigilant against cyberattacks aimed at stealing their customer's personal information and other business data that can help identity thieves.

The IRS continues to see instances where small businesses and others face a variety of identity theft related schemes that try to obtain information that can be used to file fake business tax returns. For example, phishing schemes continue to target businesses as well as tax professionals and individual taxpayers. And businesses continue to be targets of Form W-2 scams where identity thieves try to trick company leaders into sharing sensitive data.

Businesses are encouraged to follow best practices from the Federal Trade Commission, including:

- Set security software to update automatically.
- Back up important files.
- Require strong passwords for all devices.
- Encrypt devices.
- Use multi-factor authentication.

More information is available at FTC's Cybersecurity for Small Businesses.